05-2103 DC,DISTRICT-WIDE

WAGE DETERMINATION NO: 05-2103 REV (02) AREA: DC,DISTRICT-WIDE

HEALTH AND WELFARE LEVEL - INSURANCE ONLY **OTHER WELFARE LEVEL WD:05-2104

****

REGISTER OF WAGE DETERMINATIONS UNDER THE SERVICE CONTRACT ACT
By direction of the Secretary of Labor

U.S. DEPARTMENT OF LABOR
EMPLOYMENT STANDARDS ADMINISTRATION
WAGE AND HOUR DIVISION
WASHINGTON D.C. 20210

Wage Determination No.: 2005-2103
Revision No.: 2
Date Of Revision: 11/07/2006

William W.Gross
Director
Division of Wage Determinations

States: District of Columbia, Maryland, Virginia

Area: District of Columbia Statewide
Maryland Counties of Calvert, Charles, Frederick, Montgomery, Prince George's, St Mary's
Virginia Counties of Alexandria, Arlington, Fairfax, Falls Church, Fauquier, King George, Loudoun, Prince William, Stafford

Fringe Benefits Required Follow the Occupational Listing

OCCUPATION CODE - TITLE	MINIMUM WAGE RATE
01000 - Administrative Support And Clerical Occupations	
01011 - Accounting Clerk I	13.79
01012 - Accounting Clerk II	15.49
01013 - Accounting Clerk III	17.32
01020 - Administrative Assistant	21.45
01040 - Court Reporter	17.49
01051 - Data Entry Operator I	12.67

01052 - Data Entry Operator II
13.82
01060 - Dispatcher, Motor Vehicle
16.50
01070 - Document Preparation Clerk
12.75
01090 - Duplicating Machine Operator
12.75
01111 - General Clerk I
13.72
01112 - General Clerk II
15.32
01113 - General Clerk III
18.74
01120 - Housing Referral Assistant
20.84
01141 - Messenger Courier
10.23
01191 - Order Clerk I
14.74
01192 - Order Clerk II
16.29
01261 - Personnel Assistant (Employment) I
15.45
01262 - Personnel Assistant (Employment) II
17.49
01263 - Personnel Assistant (Employment) III
20.84
01270 - Production Control Clerk
20.78
01280 - Receptionist
12.29
01290 - Rental Clerk
15.45
01300 - Scheduler, Maintenance
15.45
01311 - Secretary I
16.11
01312 - Secretary II
17.61
01313 - Secretary III
20.84
01320 - Service Order Dispatcher
15.82
01410 - Supply Technician
21.45
01420 - Survey Worker
17.49
01531 - Travel Clerk I
11.69
01532 - Travel Clerk II
12.57
01533 - Travel Clerk III
13.50

01611 - Word Processor I
13.76
01612 - Word Processor II
15.45
01613 - Word Processor III
17.49
05000 - Automotive Service Occupations
05005 - Automobile Body Repairer, Fiberglass
24.49
05010 - Automotive Electrician
19.43
05040 - Automotive Glass Installer
18.31
05070 - Automotive Worker
18.31
05110 - Mobile Equipment Servicer
15.74
05130 - Motor Equipment Metal Mechanic
20.48
05160 - Motor Equipment Metal Worker
18.31
05190 - Motor Vehicle Mechanic
20.48
05220 - Motor Vehicle Mechanic Helper
16.81
05250 - Motor Vehicle Upholstery Worker
17.88
05280 - Motor Vehicle Wrecker
18.31
05310 - Painter, Automotive
19.43
05340 - Radiator Repair Specialist
18.31
05370 - Tire Repairer
14.43
05400 - Transmission Repair Specialist
20.48
07000 - Food Preparation And Service Occupations
07010 - Baker
13.18
07041 - Cook I
11.88
07042 - Cook II
13.18
07070 - Dishwasher
9.76
07130 - Food Service Worker
10.25
07210 - Meat Cutter
16.07
07260 - Waiter/Waitress
8.59
09000 - Furniture Maintenance And Repair Occupations
09010 - Electrostatic Spray Painter

18.05
09040 - Furniture Handler
12.55
09080 - Furniture Refinisher
18.05
09090 - Furniture Refinisher Helper
13.85
09110 - Furniture Repairer, Minor
16.01
09130 - Upholsterer
18.05
11000 - General Services And Support Occupations
11030 - Cleaner, Vehicles
9.67
11060 - Elevator Operator
9.79
11090 - Gardener
15.70
11122 - Housekeeping Aide
10.89
11150 - Janitor
10.89
11210 - Laborer, Grounds Maintenance
11.81
11240 - Maid or Houseman
10.41
11260 - Pruner
10.89
11270 - Tractor Operator
14.19
11330 - Trail Maintenance Worker
11.81
11360 - Window Cleaner
11.31
12000 - Health Occupations
12010 - Ambulance Driver
16.06
12011 - Breath Alcohol Technician
16.06
12012 - Certified Occupational Therapist Assistant
19.99
12015 - Certified Physical Therapist Assistant
19.99
12020 - Dental Assistant
16.90
12025 - Dental Hygienist
40.68
12030 - EKG Technician
24.34
12035 - Electroneurodiagnostic Technologist
24.34
12040 - Emergency Medical Technician
16.06
12071 - Licensed Practical Nurse I

17.15
12072 - Licensed Practical Nurse II
19.18
12073 - Licensed Practical Nurse III
21.38
12100 - Medical Assistant
14.23
12130 - Medical Laboratory Technician
16.96
12160 - Medical Record Clerk
14.96
12190 - Medical Record Technician
16.47
12195 - Medical Transcriptionist
14.96
12210 - Nuclear Medicine Technologist
28.69
12221 - Nursing Assistant I
9.37
12222 - Nursing Assistant II
10.53
12223 - Nursing Assistant III
12.18
12224 - Nursing Assistant IV
13.68
12235 - Optical Dispenser
15.15
12236 - Optical Technician
13.10
12250 - Pharmacy Technician
14.32
12280 - Phlebotomist
13.68
12305 - Radiologic Technologist
27.61
12311 - Registered Nurse I
24.92
12312 - Registered Nurse II
31.22
12313 - Registered Nurse II, Specialist
31.22
12314 - Registered Nurse III
37.77
12315 - Registered Nurse III, Anesthetist
37.77
12316 - Registered Nurse IV
45.28
12317 - Scheduler (Drug and Alcohol Testing)
17.57
13000 - Information And Arts Occupations
13011 - Exhibits Specialist I
17.98
13012 - Exhibits Specialist II
23.33

13013 - Exhibits Specialist III
28.07
13041 - Illustrator I
18.73
13042 - Illustrator II
23.42
13043 - Illustrator III
28.82
13047 - Librarian
24.54
13050 - Library Aide/Clerk
11.38
13054 - Library Information Technology Systems Administrator
22.15
13058 - Library Technician
17.88
13061 - Media Specialist I
15.99
13062 - Media Specialist II
17.88
13063 - Media Specialist III
19.94
13071 - Photographer I
14.67
13072 - Photographer II
17.18
13073 - Photographer III
21.52
13074 - Photographer IV
26.05
13075 - Photographer V
29.15
13110 - Video Teleconference Technician
15.99
14000 - Information Technology Occupations
14041 - Computer Operator I
15.45
14042 - Computer Operator II
17.49
14043 - Computer Operator III
19.50
14044 - Computer Operator IV
21.67
14045 - Computer Operator V
24.00
14071 - Computer Programmer I (1)
21.60
14072 - Computer Programmer II (1)
25.66
14073 - Computer Programmer III (1)
27.62
14074 - Computer Programmer IV (1)
27.62
14101 - Computer Systems Analyst I (1)

27.62
14102 - Computer Systems Analyst II (1)
27.62
14103 - Computer Systems Analyst III (1)
27.62
14150 - Peripheral Equipment Operator
15.45
14160 - Personal Computer Support Technician
21.67
15000 - Instructional Occupations
15010 - Aircrew Training Devices Instructor (Non-Rated)
34.39
15020 - Aircrew Training Devices Instructor (Rated)
40.64
15030 - Air Crew Training Devices Instructor (Pilot)
46.05
15050 - Computer Based Training Specialist / Instructor
31.26
15060 - Educational Technologist
27.99
15070 - Flight Instructor (Pilot)
46.05
15080 - Graphic Artist
23.02
15090 - Technical Instructor
21.70
15095 - Technical Instructor/Course Developer
26.54
15110 - Test Proctor
17.31
15120 - Tutor
17.31
16000 - Laundry, Dry-Cleaning, Pressing And Related Occupations
16010 - Assembler
8.71
16030 - Counter Attendant
8.71
16040 - Dry Cleaner
11.10
16070 - Finisher, Flatwork, Machine
8.71
16090 - Presser, Hand
8.71
16110 - Presser, Machine, Drycleaning
8.71
16130 - Presser, Machine, Shirts
8.71
16160 - Presser, Machine, Wearing Apparel, Laundry
8.71
16190 - Sewing Machine Operator
11.90
16220 - Tailor
12.63
16250 - Washer, Machine

9.44
19000 - Machine Tool Operation And Repair Occupations
  19010 - Machine-Tool Operator (Tool Room)
18.95
  19040 - Tool And Die Maker
23.05
21000 - Materials Handling And Packing Occupations
  21020 - Forklift Operator
16.25
  21030 - Material Coordinator
20.54
  21040 - Material Expediter
20.54
  21050 - Material Handling Laborer
12.65
  21071 - Order Filler
13.21
  21080 - Production Line Worker (Food Processing)
16.25
  21110 - Shipping Packer
14.46
  21130 - Shipping/Receiving Clerk
14.46
  21140 - Store Worker I
9.96
  21150 - Stock Clerk
14.35
  21210 - Tools And Parts Attendant
16.99
  21410 - Warehouse Specialist
16.25
23000 - Mechanics And Maintenance And Repair Occupations
  23010 - Aerospace Structural Welder
23.35
  23021 - Aircraft Mechanic I
22.24
  23022 - Aircraft Mechanic II
23.35
  23023 - Aircraft Mechanic III
24.52
  23040 - Aircraft Mechanic Helper
15.10
  23050 - Aircraft, Painter
21.29
  23060 - Aircraft Servicer
17.82
  23080 - Aircraft Worker
18.09
  23110 - Appliance Mechanic
20.60
  23120 - Bicycle Repairer
14.43
  23125 - Cable Splicer
24.77

23130 - Carpenter, Maintenance
20.36
23140 - Carpet Layer
18.70
23160 - Electrician, Maintenance
24.85
23181 - Electronics Technician Maintenance I
21.36
23182 - Electronics Technician Maintenance II
22.80
23183 - Electronics Technician Maintenance III
24.02
23260 - Fabric Worker
17.90
23290 - Fire Alarm System Mechanic
21.46
23310 - Fire Extinguisher Repairer
16.50
23311 - Fuel Distribution System Mechanic
22.81
23312 - Fuel Distribution System Operator
19.38
23370 - General Maintenance Worker
19.01
23380 - Ground Support Equipment Mechanic
22.24
23381 - Ground Support Equipment Servicer
17.82
23382 - Ground Support Equipment Worker
18.09
23391 - Gunsmith I
16.50
23392 - Gunsmith II
19.18
23393 - Gunsmith III
21.46
23410 - Heating, Ventilation And Air-Conditioning Mechanic
20.99
23411 - Heating, Ventilation And Air Contditioning Mechanic (Research Facility)
22.12
23430 - Heavy Equipment Mechanic
21.46
23440 - Heavy Equipment Operator
21.46
23460 - Instrument Mechanic
21.46
23465 - Laboratory/Shelter Mechanic
20.36
23470 - Laborer
14.27
23510 - Locksmith
19.17
23530 - Machinery Maintenance Mechanic

21.46
23550 - Machinist, Maintenance
21.52
23580 - Maintenance Trades Helper
15.10
23591 - Metrology Technician I
21.46
23592 - Metrology Technician II
22.61
23593 - Metrology Technician III
23.72
23640 - Millwright
23.30
23710 - Office Appliance Repairer
20.36
23760 - Painter, Maintenance
20.36
23790 - Pipefitter, Maintenance
22.76
23810 - Plumber, Maintenance
20.99
23820 - Pneudraulic Systems Mechanic
21.46
23850 - Rigger
21.46
23870 - Scale Mechanic
19.18
23890 - Sheet-Metal Worker, Maintenance
21.46
23910 - Small Engine Mechanic
20.05
23931 - Telecommunications Mechanic I
24.43
23932 - Telecommunications Mechanic II
25.75
23950 - Telephone Lineman
22.21
23960 - Welder, Combination, Maintenance
21.46
23965 - Well Driller
21.46
23970 - Woodcraft Worker
21.46
23980 - Woodworker
16.50
24000 - Personal Needs Occupations
24570 - Child Care Attendant
11.58
24580 - Child Care Center Clerk
16.15
24610 - Chore Aide
9.58
24620 - Family Readiness And Support Services Coordinator
12.95

24630 - Homemaker
16.75
25000 - Plant And System Operations Occupations
25010 - Boiler Tender
24.06
25040 - Sewage Plant Operator
20.08
25070 - Stationary Engineer
24.06
25190 - Ventilation Equipment Tender
16.76
25210 - Water Treatment Plant Operator
20.08
27000 - Protective Service Occupations
27004 - Alarm Monitor
17.19
27007 - Baggage Inspector
11.51
27008 - Corrections Officer
18.75
27010 - Court Security Officer
21.42
27030 - Detection Dog Handler
16.67
27040 - Detention Officer
18.75
27070 - Firefighter
21.58
27101 - Guard I
11.51
27102 - Guard II
16.67
27131 - Police Officer I
23.94
27132 - Police Officer II
26.60
28000 - Recreation Occupations
28041 - Carnival Equipment Operator
12.35
28042 - Carnival Equipment Repairer
13.30
28043 - Carnival Equpment Worker
8.40
28210 - Gate Attendant/Gate Tender
12.68
28310 - Lifeguard
11.29
28350 - Park Attendant (Aide)
14.18
28510 - Recreation Aide/Health Facility Attendant
10.35
28515 - Recreation Specialist
17.57
28630 - Sports Official

11.29
28690 - Swimming Pool Operator
15.32
29000 - Stevedoring/Longshoremen Occupational Services
29010 - Blocker And Bracer
20.55
29020 - Hatch Tender
20.55
29030 - Line Handler
20.55
29041 - Stevedore I
19.18
29042 - Stevedore II
21.64
30000 - Technical Occupations
30010 - Air Traffic Control Specialist, Center (HFO) (2)
33.82
30011 - Air Traffic Control Specialist, Station (HFO) (2)
23.32
30012 - Air Traffic Control Specialist, Terminal (HFO) (2)
25.68
30021 - Archeological Technician I
16.92
30022 - Archeological Technician II
18.85
30023 - Archeological Technician III
23.53
30030 - Cartographic Technician
24.62
30040 - Civil Engineering Technician
22.19
30061 - Drafter/CAD Operator I
17.77
30062 - Drafter/CAD Operator II
19.87
30063 - Drafter/CAD Operator III
22.15
30064 - Drafter/CAD Operator IV
25.66
30081 - Engineering Technician I
18.80
30082 - Engineering Technician II
21.11
30083 - Engineering Technician III
23.61
30084 - Engineering Technician IV
29.26
30085 - Engineering Technician V
35.26
30086 - Engineering Technician VI
43.30
30090 - Environmental Technician
21.22
30210 - Laboratory Technician

20.42
30240 - Mathematical Technician
24.62
30361 - Paralegal/Legal Assistant I
20.03
30362 - Paralegal/Legal Assistant II
24.82
30363 - Paralegal/Legal Assistant III
30.35
30364 - Paralegal/Legal Assistant IV
36.73
30390 - Photo-Optics Technician
24.62
30461 - Technical Writer I
20.25
30462 - Technical Writer II
24.77
30463 - Technical Writer III
29.97
30491 - Unexploded Ordnance (UXO) Technician I
21.49
30492 - Unexploded Ordnance (UXO) Technician II
26.00
30493 - Unexploded Ordnance (UXO) Technician III
31.17
30494 - Unexploded (UXO) Safety Escort
21.49
30495 - Unexploded (UXO) Sweep Personnel
21.49
30620 - Weather Observer, Combined Upper Air Or Surface Programs (3)
20.13
30621 - Weather Observer, Senior (3)
21.80
31000 - Transportation/Mobile Equipment Operation Occupations
31020 - Bus Aide
10.90
31030 - Bus Driver
15.95
31043 - Driver Courier
12.71
31260 - Parking and Lot Attendant
8.67
31290 - Shuttle Bus Driver
13.89
31310 - Taxi Driver
13.98
31361 - Truckdriver, Light
13.89
31362 - Truckdriver, Medium
17.09
31363 - Truckdriver, Heavy
18.40
31364 - Truckdriver, Tractor-Trailer
18.40

99000 - Miscellaneous Occupations
  99030 - Cashier
10.03
  99050 - Desk Clerk
9.78
  99095 - Embalmer
21.77
  99251 - Laboratory Animal Caretaker I
10.47
  99252 - Laboratory Animal Caretaker II
10.85
  99310 - Mortician
27.25
  99410 - Pest Controller
13.74
  99510 - Photofinishing Worker
11.29
  99710 - Recycling Laborer
14.50
  99711 - Recycling Specialist
17.02
  99730 - Refuse Collector
12.86
  99810 - Sales Clerk
11.13
  99820 - School Crossing Guard
11.37
  99830 - Survey Party Chief
19.16
  99831 - Surveying Aide
11.91
  99832 - Surveying Technician
18.21
  99840 - Vending Machine Attendant
11.46
  99841 - Vending Machine Repairer
14.88
  99842 - Vending Machine Repairer Helper
11.46

ALL OCCUPATIONS LISTED ABOVE RECEIVE THE FOLLOWING BENEFITS:

HEALTH & WELFARE: $3.01 per hour or $120.40 per week or $521.73 per month

VACATION: 2 weeks paid vacation after 1 year of service with a contractor or
successor; 3 weeks after 5 years, and 4 weeks after 15 years. Length of service
includes the whole span of continuous service with the present

contractor or
successor, wherever employed, and with the predecessor contractors in the
performance of similar work at the same Federal facility. (Reg. 29 CFR 4.173)

HOLIDAYS: HOLIDAYS: A minimum of ten paid holidays per year, New Year's Day,
Martin Luther King Jr's Birthday, Washington's Birthday, Memorial Day,
Independence Day, Labor Day, Columbus Day, Veterans' Day, Thanksgiving Day, and
Christmas Day. (A contractor may substitute for any of the named holidays another
day off with pay in accordance with a plan communicated to the employees involved.)
(See 29 CFR 4174)

THE OCCUPATIONS WHICH HAVE PARENTHESES AFTER THEM RECEIVE THE FOLLOWING BENEFITS (as
numbered):

1) Does not apply to employees employed in a bona fide executive, administrative,
or professional capacity as defined and delineated in 29 CFR 541. (See CFR 4.156)

2) APPLICABLE TO AIR TRAFFIC CONTROLLERS ONLY - NIGHT DIFFERENTIAL: An employee is
entitled to pay for all work performed between the hours of 6:00 P.M. and 6:00 A.M.
at the rate of basic pay plus a night pay differential amounting to 10 percent of
the rate of basic pay.

3) WEATHER OBSERVERS - NIGHT PAY & SUNDAY PAY: If you work at night as part of a
regular tour of duty, you will earn a night differential and receive an additional
10% of basic pay for any hours worked between 6pm and 6am. If you are a full-time
employed (40 hours a week) and Sunday is part of your regularly scheduled workweek,
you are paid at your rate of basic pay plus a Sunday premium of 25% of your basic
rate for each hour of Sunday work which is not overtime (i.e. occasional work on
Sunday outside the normal tour of duty is considered overtime work).

HAZARDOUS PAY DIFFERENTIAL: An 8 percent differential is applicable to employees
employed in a position that represents a high degree of hazard when

working with or
in close proximity to ordinance, explosives, and incendiary materials. This
includes work such as screening, blending, dying, mixing, and pressing of sensitive
ordance, explosives, and pyrotechnic compositions such as lead azide, black powder
and photoflash powder. All dry-house activities involving propellants or
explosives. Demilitarization, modification, renovation, demolition, and maintenance
operations on sensitive ordnance, explosives and incendiary materials. All
operations involving regrading and cleaning of artillery ranges.

A 4 percent differential is applicable to employees employed in a position that
represents a low degree of hazard when working with, or in close proximity to
ordance, (or employees possibly adjacent to) explosives and incendiary materials
which involves potential injury such as laceration of hands, face, or arms of the
employee engaged in the operation, irritation of the skin, minor burns and the
like; minimal damage to immediate or adjacent work area or equipment being used.
All operations involving, unloading, storage, and hauling of ordance, explosive, and
incendiary ordnance material other than small arms ammunition. These differentials
are only applicable to work that has been specifically designated by the agency for
ordance, explosives, and incendiary material differential pay.

** UNIFORM ALLOWANCE **

If employees are required to wear uniforms in the performance of this contract
(either by the terms of the Government contract, by the employer, by the state or
local law, etc.), the cost of furnishing such uniforms and maintaining (by
laundering or dry cleaning) such uniforms is an expense that may not be borne by an
employee where such cost reduces the hourly rate below that required by the wage
determination. The Department of Labor will accept payment in accordance with the
following standards as compliance:

The contractor or subcontractor is required to furnish all employees with an
adequate number of uniforms without cost or to reimburse employees for

the actual
cost of the uniforms. In addition, where uniform cleaning and maintenance is made
the responsibility of the employee, all contractors and subcontractors subject to
this wage determination shall (in the absence of a bona fide collective bargaining
agreement providing for a different amount, or the furnishing of contrary
affirmative proof as to the actual cost), reimburse all employees for such cleaning
and maintenance at a rate of $3.35 per week (or $.67 cents per day). However, in
those instances where the uniforms furnished are made of "wash and wear"
materials, may be routinely washed and dried with other personal garments, and do
not require any special treatment such as dry cleaning, daily washing, or commercial
laundering in order to meet the cleanliness or appearance standards set by the terms
of the Government contract, by the contractor, by law, or by the nature of the work,
there is no requirement that employees be reimbursed for uniform maintenance costs.

The duties of employees under job titles listed are those described in the
"Service Contract Act Directory of Occupations," Fifth Edition, April 2006,
unless otherwise indicated. Copies of the Directory are available on the Internet. A
links to the Directory may be found on the WHD home page at
<http://www.dol.gov/esa/whd/> or through the Wage Determinations On-Line (WDOL) Web
site at <http://wdol.gov/>.

REQUEST FOR AUTHORIZATION OF ADDITIONAL CLASSIFICATION AND WAGE RATE {Standard Form
1444 (SF 1444)}

Conformance Process:

The contracting officer shall require that any class of service employee which is
not listed herein and which is to be employed under the contract (i.e., the work to
be performed is not performed by any classification listed in the wage
determination), be classified by the contractor so as to provide a reasonable
relationship (i.e., appropriate level of skill comparison) between such unlisted
classifications and the classifications listed in the wage determination. Such
conformed classes of employees shall be paid the monetary wages and

furnished the
fringe benefits as are determined. Such conforming process shall be initiated by
the contractor prior to the performance of contract work by such unlisted class(es)
of employees. The conformed classification, wage rate, and/or fringe benefits shall
be retroactive to the commencement date of the contract. {See Section 4.6 (C)(vi)}
When multiple wage determinations are included in a contract, a separate SF 1444
should be prepared for each wage determination to which a class(es) is to be
conformed.

The process for preparing a conformance request is as follows:

1) When preparing the bid, the contractor identifies the need for a conformed
occupation) and computes a proposed rate).

2) After contract award, the contractor prepares a written report listing in order
proposed classification title), a Federal grade equivalency (FGE) for each
proposed classification), job description), and rationale for proposed wage
rate), including information regarding the agreement or disagreement of the
authorized representative of the employees involved, or where there is no authorized
representative, the employees themselves. This report should be submitted to the
contracting officer no later than 30 days after such unlisted class(es) of employees
performs any contract work.

3) The contracting officer reviews the proposed action and promptly submits a report
of the action, together with the agency's recommendations and pertinent
information including the position of the contractor and the employees, to the Wage
and Hour Division, Employment Standards Administration, U.S. Department of Labor,
for review. (See section 4.6(b)(2) of Regulations 29 CFR Part 4).

4) Within 30 days of receipt, the Wage and Hour Division approves, modifies, or
disapproves the action via transmittal to the agency contracting officer, or
notifies the contracting officer that additional time will be required to process
the request.

5) The contracting officer transmits the Wage and Hour decision to the contractor.

6) The contractor informs the affected employees.

Information required by the Regulations must be submitted on SF 1444 or bond paper.

When preparing a conformance request, the "Service Contract Act Directory of Occupations" (the Directory) should be used to compare job definitions to insure that duties requested are not performed by a classification already listed in the wage determination. Remember, it is not the job title, but the required tasks that determine whether a class is included in an established wage determination. Conformances may not be used to artificially split, combine, or subdivide classifications listed in the wage determination.

YOUR LETTERHEAD

EQUAL EMPLOYMENT OPPORTUNITY (EEO) POLICY STATEMENT

_____SHALL NOT DISCRIMINATE AGAINST ANY EMPLOYEE OR APPLICANT FOR EMPLOYMENT BECAUSE OF RACE, COLOR, RELIGION, NATIONAL ORIGIN, SEX, AGE, MARITIAL STATUS, PERSONAL APPEARANCE, SEXUAL ORIENTATION, FAMILY RESPONSIBILITIES, MATRICULATION, POLITICAL AFFILIATION, OR PHYSICAL HANDICAP.

_____AGREES TO AFIRMATIVE ACTION TO ENSURE THAT APPLICANTS ARE EMPLOYED, AND THAT EMPLOYEES ARE TREATED DURING EMPLOYMENT, WITHOUT REGARD TO THEIR RACE, COLOR, RELIGION, NATIONAL ORIGIN, SEX, AGE, MARITIAL STATUS, PERSONAL APPEARANCE, SEXUAL ORIENTATION, FAMILY RESPONSIBILITIES, MATRICULATION, POLITICAL AFFILIATION, OR PHYSICAL HANDICAP.THE AFFIRMATIVE ACTION SHALL INCLUDE, BUT NOT BE LIMITED TO THE FOLLOWING: (A) EMPLOYMENT, UPGRADING, OR TRANSFER; (B) RECRUITMENT OR RECRUITMENT ADVERTISING; (C) DEMOTION, LAYOFF, OR TERMINATION; (D) RATES OF PAY, OR OTHER FORMS OF COMPENSATION; AND (E) SELECTION FOR TRAINING AND APPRENTICESHIP.

_____AGREES TO POST IN CONSPICUOUS PLACES THE PROVISIONS CONCERNING NON-DISCRIMINATION AND AFFIRMATIVE ACTION.

_____SHALL STATE THAT ALL QUALIFIED APPLICANTS WILL RECEIVE CONSIDERATION FOR EMPLOYMENT PURSUANT TO SUBSECTION 1103.2 THROUGH 1103.10 OF MAYOR' S ORDER 85-85; "EQUAL EMPLOYMENT OPPORTUNITY REQUIREMENTS IN CONTRACTS."

_____AGREES TO PERMIT ACCESS TO ALL BOOKS PERTAINING TO ITS EMPLOYMENT PRACTICES, AND TO REQUIRE EACH SUBCONTRACTOR TO PERMIT ACCESS TO BOOKS AND RECORDS.

_____AGREES TO COMPLY WITH ALL GUIDELINES FOR EQUAL EMPLOYMENT OPPORTUNITY APPLICABLE IN THE DISTRICT OF COLUMBIA.

_____SHALL INCLUDE IN EVERY SUBCONTRACT THE EQUAL OPPORTUNITY CLAUSES, SUBSECTION 1103.2 THROUGH 1103.10 SO THAT SUCH PROVISIONS SHALL BE BINDING UPON EACH SUBCONTRACTOR OR VENDOR.

_____
AUTHORIZED OFFICIAL AND TITLE

_____
AUTHORIZED SIGNATURE

_____
FIRM/ORGA NIZATION NAME

_____
DATE

YOUR LETTERHEAD

ASSURANCE OF COMPLIANCE WITH EQUAL EMPLOYMENT OPPORTUNITY REQUIREMENTS

MAYOR'S ORDER 85-85, EFFECTIVE JUNE 10, 1985, AND THE RULES IMPLEMENTING MAYORS ORDER 85-85, 33 DCR 4952, (PUBLISHED AUGUST 15, 1986), "ON COMPLIANCE WITH EQUAL OPPORTUNITY REQUIREMENTS IN DISTRICT GOVERNMENT CONTRACTS," ARE HEREBY INCLUDED AS PART OF THIS BID/PROPOSAL. THEREFORE, EACH BIDDER/OFFEROR SHALL INDICATE BELOW THEIR WRITTEN COMMITMENT TO ASSURE COMPLIANCE WITH MAYOR'S ORDER 85-85 AND THE IMPLEMENTING RULES. FAILURE TO COMPLY WITH THE SUBJECT MAYOR'S ORDER AND THE IMPLEMENTING RULES SHALL RESULT IN REJECTION OF THE RESPECTIVE BID/PROPOSAL.

I, _____, THE AUTHORIZED REPRESENTATIVE OF _____, HEREINAFTER REFERRED TO AS "THE CONTRACTOR," CERTIFY THT THE CONTRATOR IS FULLY AWARE OF ALL OF THE PROVISIONS OF MAYOR'S ORDER 85-85, EFFECTIVE JUNE 10, 1985, AND OF THE RULES IMPLEMENTING MAYOR'S ORDER 85-85, 33 DCR 4952. I FURTHER CERTIFY AND ASSURE THAT THE CONTRACTOR WILL FULLY COMPLY WITH ALL APPLICABLE PROVISIONS OF THE MAYOR'S ORDER AND IMPLEMENTING RULES IF AWARDED THE D.C. GOVERNMENT REFERENCED BY THE CONTRACT NUMBER ENTERED BELOW. FURTHER, THE CONTRACTOR ACKNOWLEDGES AND UNDERSTANDS THAT THE AWARD OF SAID CONTRACT AND ITS CONTINUATION ARE SPECIFICALLY CONDITIONED UPON THE CONTRACTOR'S COMPLIANCE WITH THE ABOVE-CITED ORDER AND RULES.

_____
CONTRACTOR

_____
NAME

_____
SIGNATURE

_____
TITLE

_____
CONTRACT NUMBER

_____
DATE

EQUAL EMPLOYMENT OPPORTUNITY
EMPLOYER INFORMATION REPORT

GOVERNMENT OF THE DISTRICT OF COLUMBIA DC Office of Contracting and Procurement Employer Information Report (EEO)	Reply to: Office of Contracting and Procurement 441 4th Street, NW, Suite 700 South Washington, DC 20001

Instructions:
Two (2) copies of DAS 84-404 or Federal Form EEO-1 shall be submitted to the Office of Contracting and Procurement.
One copy shall be retained by the Contractor.

Section A – TYPE OF REPORT

1. Indicate by marking in the appropriate box the type of reporting unit for which this copy of the form is submitted (MARK ONLY ONE BOX)

Single Establishment Employer	Multi-establishment Employer:
(1) Single-establishment Employer Report	(2) ÿ Consolidated Report (3) ÿ Headquarters Report (4) ÿ Individual Establishment Report (submit one for each establishment with 25 or more employees) (5) ÿ Special Report

1. Total number of reports being filed by this Company. _____

Section B – COMPANY IDENTIFICATION (*To be answered by all employers)*

					OFFICIAL USE ONLY
1. Name of Company which owns or controls the establishment for which this report is filed					a.
Address (Number and street)	City or Town	Country	State	Zip Code	b.
b. Employer Identification No.					
2. Establishment for which this report is filed.					OFFICIAL USE ONLY
a. Name of establishment					c.
Address (Number and street)	City or Town	Country	State	Zip Code	d.
b. Employer Identification No.					
3. Parent of affiliated Company					
a. Name of parent or affiliated Company	b. Employer Identification No.				
Address (Number and Street)	City or Town	Country	State	Zip Code	

Section C - ESTABLISHMENT INFORMATION

1. Is the location of the establishment the same as that reported last year? Yes No Did not report last year Report on combined basis	2. Is the major business activity at this establishment the same as that reported last year? Yes No No report last year Reported on combined basis	OFFICIAL USE ONLY
2. What is the major activity of this establishment? (Be specific, i.e., manufacturing steel castings, retail grocer, wholesale plumbing supplies, title insurance, etc. Include the specific type of product or service provided, as well as the principal business or industrial activity.		e.

3. MINORITY GROUP MEMBERS: Indicate if you are a minority business enterprise (50% owned or 51% controlled by minority members).

Yes No

DAS 84-404 (Replaces D.C. Form 2640.9 Sept. 74 which is Obsolete) 84-2P891

SECTION D – EMPLOYMENT DATA

Employment at this establishment – Report all permanent, temporary, or part-time employees including apprentices and on-the-job trainees unless specifically excluded as set forth in the instructions. Enter the appropriate figures on all lines and in all columns. Blank spaces will be considered as zero. *In columns 1, 2, and 3, include ALL employees in the establishment including those in minority groups*

JOB CATEGORIES	TOTAL EMPLOYEES IN ESTABLISHMENT			MINORITY GROUP EMPLOYEES							
				MALE				FEMALE			
	Total Employees Including Minorities (1)	Total Male Including Minorities (2)	Total Female Including Minorities (3)	Black (4)	Oriental (5)	American Indian (6)	Spanish Surname American (7)	Black (8)	Oriental (9)	American Indian (10)	Spanish Surname American (11)
Officials and Managers											
Professionals											
Technicians											
Sales Workers											
Office and Clerical											
Craftsman (Skilled)											
Operative (Semi-Skilled)											
Laborers (Unskilled)											
Service Workers											
TOTAL											
Total employ reported in previous report											

(The trainee below should also be included in the figures for the appropriate occupation categories above)

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Formal On-The-Job Trainee	White collar											
	Production											

1. How was information as to race or ethnic group in Section D obtained?
   a. Visual Survey
   b. Employment Record
   c. Other Specify _____
   _____
2. Dates of payroll period used
3. Pay period of last report submitted for this establishment._____

Section E – REMARKS Use this Item to give any identification data appearing on last report which differs from that given above, explain major changes in composition or reporting units, and other pertinent information.

Section F - CERTIFICATION

Check One
1. All reports are accurate and were prepared in accordance with the instructions (check on consolidated only)
2. This report is accurate and was prepared in accordance with the instructions.

Name of Authorized Official | Title | Signature | Date

Name of person contact regarding This report (Type of print) | Address (Number and street)

Title | City and State | Zip Code | Telephone Number | Extension

INFORMATION CITED HEREIN SHALL BE HELD IN CONFIDENCE.

DEPARTMENT OF HUMAN RIGHTS AND LOCAL BUSINESS DEVELOPMENT
CONTRACT COMPLIANCE UNIT

SUBCONTRACT SUMMARY FORM

This SUMMARY form is to be completed by the PRIME contractor.

BID NO.: CCB NUMBER: _____ of _____ pages

*NOTE: The standard for minority subcontracting is 25% of the TOTAL contract dollar amount to be subcontracted.

AMOUNT OF PRIME CONTRACT: $_____
AMOUNT OF ALL SUBCONTRACTS: $_____ equals _____% OF THE PRIME CONTRACT.

NAME OF PRIME CONTRACTOR:

TELEPHONE NO.

ADDRESS:

PROJECT NAME:
ADDRESS:

WARD NO.: _____

PROJECT DESCRIPTIONS:

SECTION II LIST ALL SUBCONTRACTORS THAT WILL BE UTILIZED ON THE ABOVE PROJECT

1. NAME OF SUBCONTRACTOR 2. ADDRESS 3. CONTACT PERSON 4. MBOC CERT. NO.	5. PHONE NO.	1. IS THIS A *MINORITY SUB? _____ YES _____ NO 2. TRADE OR BUSINESS PRODUCT THAT SUB WILL PROVIDE.	1. $ AMOUNT OF SUBCONTRACT equals(=) 2. _____% (percent) OF TOTAL PRIME CONTRACT.
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%
1. 2. 3. 4.	5.	1. MINORITY SUBCONTRACTOR _____ YES _____ NO 2.	1. $_____ equals(=) 2. _____%

TOTAL DOLLAR AMOUNT SUBCONTRACTED TO *MINORITY BUSINESS ENTERPRISES. $_____

PERCENT OF PRIME CONTRACT. _____%

*D.C. LAW 1-95, as amended, defines a **MINORITY BUSINESS ENTERPRISE** as a business of which more than 50% is owned by members of a minority, and of which more than 50% of the net profit or loss accrues to members of a minority.

SOLICITATION NO: _____

PROJECTED GOALS AND TIMETABLES FOR FUTURE HIRING

JOB CATEGORIES	MINORITY GROUP EMLOYES GOALS								TIMETABLES
	MALE				FEMALE				
	BLACK	ASIAN	AMERICAN INDIAN	HISPANIC	BLACK	ASIAN	AMERICAN INDIAN	HISPANIC	
OFFICIALS & MANAGERS									
PROFESSIONALS									
TECHNICIANS									
SALES WORKERS									
OFFICE AND CLERICAL									
CRAFTSMANS (SKILLELD)									
OPERATIVE (SEMI-SKILLED)									
LABORERS (UNSKILLED)									
SERVICE WORKERS									
TOTALS									

NAME OF AUTHORIZED OFFICIAL:	TITLE:	SIGNATURE:
FIRM NAME:	TELEHONE NO:	DATE:

INDICATE IF THE PRIME UTILIZES A "MINORITY FINANCIAL INSTITUTION"

_____ Yes _____ No

NAME:

ADDRESS:

TYPE OF ACCOUNT/S:

GOVERNMENT OF THE DISTRICT OF COLUMBIA

ADMINISTRATIVE ISSUANCE SYSTEM

SUBJECT: Compliance with Equal Opportunity Obligations in Contracts

ORIGINATING AGENCY: Office of the Mayor

By virtue of the authority vested in me as Mayor of the District of Columbia by Section 422 of the District of Columbia self-government and Government Reorganization Act of 1973 as amended, D.C. Code section 1-242 (1981-Ed.), it is hereby ORDERED that Commissioner's Order No. 73-51, dated February 28, 1973, is hereby rescinded and reissued in its entirety to read as follows:

1. Establishment of Policy: There is established a policy of the District of Columbia Government to:

   (a) provide equal opportunity in employment for all persons with respect to any contract by and with the Government of the District of Columbia.

   (b) prohibit discrimination in employment because of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, family responsibilities, matriculation, political affiliation, or physical handicap;

   (c) provide equal opportunity to all persons for participation in all District of Columbia Government contracts, including but not limited to lease agreements, Industrial Revenue Bond financing, and Urban Development Action grants;

   (d) provide equal opportunity to minority business enterprises in the performance of District of Columbia Government contracts in accordance with Mayor's Orders, District of Columbia laws, and rules and regulations promulgated by the Minority Business Opportunity Commission; and

   (e) promote the full realization of equal employment through affirmative, continuing programs by contractors and subcontractors in the performance of contracts with the District of Columbia Government.

2. Delegation of Authority: The Director of the Office of Human Rights (hereinafter "Director") is delegated the authority vested in the Mayor to implement the provisions of this order as set forth herein, and any rules, regulations, guidelines, and procedures adopted pursuant thereto.

3. Responsibilities: The Director of the Office of Human Rights shall be responsible for establishing and ensuring agency compliance with the policy set forth in this Order, any rules, regulations, and procedures that may be adopted by the Office of Human Rights pursuant to this Order, and any other equal opportunity provisions as may be added as a part of any contract.

4. Powers and Duties: The Director of the Office of Human Rights shall have the following powers and duties:

   (a) to establish standards and procedures by which contractors and subcontractors who perform under District of Columbia Government contracts shall comply with the equal opportunity provisions of their contracts; to issue all orders, rules, regulations, guidelines, and procedures the Director may deem necessary and proper for carrying out and implementing the purposes of this Order;

   (b) to assume equal opportunity compliance jurisdiction over any matter pending before a contracting agency where the Director considers it necessary or appropriate for the achievement of the purposes of

this Order, keep the contracting agency informed of all actions taken, and act through the contracting agency to the extent appropriate and practicable;

(c) to examine the employment practices of any District of Columbia Government contractor or subcontractor, or initiate the examination by the appropriate contracting agency to determine whether or not the contractual provisions specified in any rules and regulations adopted pursuant to this Order have been violated, and notify the contracting agency of any action taken or recommended;

(d) to monitor and evaluate all District of Columbia Government agencies, including those independent agencies and commissions not required to submit the Affirmative Action Programs of their contractors to the Office of Human Rights for approval, to ensure compliance with the equal opportunity obligations in contracts;

(e) to use his or her best efforts to cause any labor union engaged in work under District of Columbia Government contracts, any referral, recruiting or training agency, or any other representative of workers who are or may be engaged in work under contracts and subcontracts to cooperate in and to comply with the implementation of the purposes of this Order;

(f) to notify, when appropriate, the concerned contracting agencies, the Office of Federal Contract Compliance Programs, the U.S. Department of Justice, or other appropriate Federal, State, and District agencies, whenever the Director has reason to believe that practices of any contractor, labor organization, lending institution, insurance firm, or agency violate provisions of Federal, State, or District, laws;

(g) to enter, where the determinations are made by Federal, State, or District agencies, into reciprocal agreements with those agencies to receive the appropriate information;

(h) to hold hearings, public or private, as necessary to obtain compliance with any rules, regulations, and procedures promulgated pursuant to this Order, and to issue orders relating thereto. No order to terminate or cancel a contract, or to withhold from any contractor further District of Columbia Government contractors shall be issued without affording the contractor an opportunity for a hearing. Any order to terminate or cancel a contract or to withhold from any contractor further District of Columbia Government contracts shall be issued in accordance with rules, and regulations pursuant to the Administrative Procedure Act, as amended and;

(i) to grant waivers from the minimum standards for the employment of minorities and women in Affirmative Action Programs in exceptional cases, as circumstances may warrant.

5. Duties of Contracting Agencies: Each contracting agency shall have the following duties:

(a) the initial responsibility for ensuring that contractors and subcontractors are in compliance with any rules, regulations, and procedures promulgated pursuant to this Order;

(b) to examine the employment practices of contractors and subcontractors in accordance with procedures established by the Office of Human Rights, and report any compliance action to the Director of the Office of Human Rights;

(c) to comply with the terms of this Order and of the orders, rules, regulations, guidelines, and procedures of the Office of Human Rights issued pursuant thereto in discharging their responsibility for securing contract compliance; and

(d) to secure compliance with any rules, regulations, and procedures promulgated pursuant to this Order before or after the execution of a contract by methods, of conference, conciliation and persuasion. No enforcement proceedings shall be initiated, nor shall a contract be cancelled or terminated in whole or in part, unless such methods have first been attempted.

6. Procedures: The procedures to be followed in implementing this Order shall be those set forth in

Orders, rules, regulations, and guidelines as may be promulgated by the Office of Human Rights.

7. Severability: If any section, subsection, sentence, clause, phrase, or portion of the provisions in this Order is for any reason declared by any court of competent jurisdiction to be invalid or unconstitutional, such section, subsection, sentence, clause, phrase, or portion shall be deemed a separate, distinct, and independent provision, and such holding shall not affect the validity of the remaining provisions of this order.

8. Effective Date: This Order shall become effective immediately.

Signed by Marion Barry, Jr.
Mayor

ATTEST: Signed by Clifton B. Smith
Secretary of the District of Columbia

OFFICE OF HUMAN RIGHTS

NOTICE OF FINAL RULEMAKING

The Director of the Office of Human Rights hereby gives notice of the adoption of the following final rules governing standards and procedures for equal employment opportunity applicable to contractors and subcontractors under District of Columbia Government Contracts. Notice of Proposed Rulemaking was published for public comment in the D.C. Register on April 11, 1986 at 33 DCR 2243. Based on some the comments received and upon further review by the Office of Human Rights, minor revisions were made in the rules at the following subsections: 1104.1, 1104.2, 1104.4, 1104.13, 1104.17(e) (5), 1104.28, 1107.1, 1199.1, and at page 15 the definition of minority was written out in addition to citing its D.C. Code. None of the revisions change the intent of the proposed final rules. Final action to adopt these final rules was taken on August 4, 1986, and will be effective upon publication of this notice in the Register.

CHAPTER 11 EQUAL EMPLOYMENT OPPORTUNITY REQUIREMENTS IN CONTRACTS

1100 PURPOSE

1100.1 These rules shall govern standards and procedures to be followed by contractors and subcontractors performing under District of Columbia Government contracts for goods and services, including construction contracts, for the purpose of assuring equal employment opportunity for minorities and women.

1100.2 These rules establish requirements for contractors and subcontractors regarding their commitment to observe specific standards for the employment of minorities and women and to achieve affirmative action obligations under District of Columbia contracts. These rules are not intended nor shall be used to discriminate against any qualified applicant for employment or employee.

1101 SCOPE

1101.1 Except as hereinafter exempted, the provisions of this chapter shall apply to all District of Columbia Government contracts subject to Mayor's Order No. 85-85, and any rules, regulations, and procedures promulgated pursuant to that Mayor's Order.

1102 COVERAGE

1102.1 The provisions of this chapter shall govern the processing of any matter before the Office Human Rights involving the following:

(a) Discrimination in employment on grounds of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, family responsibilities, matriculation, political affiliation, or physical handicap by any District of Columbia Government contractor; and

(b) Achievement of affirmative action obligations under District of Columbia contracts.

1103 CONTRACT PROVISIONS

1103.1 Each contract for goods and services, including construction contracts, except construction subcontracts for standard commercial supplies or raw materials, shall include as express contractual provisions the language contained in subsections 1103.2 through 1103.10.

1103.2 The contractor shall not discriminate against any employee or applicant for employment because of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, family responsibilities, matriculation, political affiliation, or physical handicap.

1103.3 The contractor agrees to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, family responsibilities, matriculation, political affiliation, or physical handicap. The affirmative action shall include, but not be limited to the following:

(a) Employment, upgrading, or transfer;
(b) Recruitment or recruitment advertising;
(c) Demotion, layoff, or termination;
(d) Rates of pay, or other forms of compensation; and
(e) Selection for training and apprenticeship.

1103.4 The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Contracting Agency, setting forth the provisions in subsections 1103.2 and 1103.3 concerning non-discrimination and affirmative action.

1103.5 The contractor shall, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment pursuant to the non-discrimination requirements set forth in subsection 1103.2

1103.6 The contractor agrees to send to each labor union or representative of workers with which it has a collective bargaining agreement, or other contract or understanding, a notice to be provided by the Contracting Agency, advising each labor union or workers' representative of the contractor's commitments under this chapter, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

1103.7 The contractor agrees to permit access to all books, records, and accounts, pertaining to its employment practices, by the Director and the Contracting Agency for purposes of investigation to ascertain compliance with this chapter, and to require under terms of any subcontractor agreement each subcontractor to permit access of such subcontractors, books, records, and accounts for such purposes.

1103.8 The contractor agrees to comply with the provisions of this chapter and with all guidelines for equal employment opportunity applicable in the District of Columbia adopted by the Director, or any authorized official.

1103.9 The prime contractor shall include in every subcontract the equal opportunity clauses, subsections 1103.2 through 1103.10 of this section, so that such provisions shall be binding upon each subcontractor or vendor.

1103.10 The prime contractor shall take such action with respect to any subcontractor as the Contracting Officer may direct as a means of enforcing these provisions, including sanctions for non-compliance; provided, however, that in the event the prime contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the contracting agency, the prime contractor may request the District to enter into such litigation to protect the interest of the District.

1104 AFFIRMATIVE ACTION PROGRAM

1104.1 Each apparent low bidder for a construction contract shall complete and submit to the Contracting Agency, prior to the execution of any contract in the amount of twenty-five thousand dollars ($25,000) or more, and each contractor covered under subsection 1105.1, an Affirmative Action Program to ensure equal opportunity which shall include specific standards for the utilization of minorities and women in the trades, crafts and skills to be used by the contractor in the performance of the contract.

1104.2 Each apparent low bidder or offeror for a non-construction contract shall complete and submit to the Contracting Agency, prior to the execution of any contract in the amount of ten thousand dollars ($10,000) or more, and each contractor covered under subsection 1105.2 , an Affirmative Action Program to ensure equal opportunity which shall include specific standards for the utilization of minorities in the job categories specified in subsection 1108.4.

1104.3 To ensure equal opportunity each Affirmative Action Program shall include the following commitments:

(a) With respect to construction contracts, each contractor shall certify that it will comply with the provisions of this chapter, and submit a personnel utilization schedule for all the trades the contractor is to utilize, indicating the actual numbers of minority and female workers that are expected to be a part of the workforce performing under the contract; and

(b) With respect to non-construction contracts, each contractor shall certify that it will comply with the provisions of this chapter, and shall submit a personnel utilization schedule indicating by craft and skill, the minority composition of the workforce related to the performance of the work under the contract. The schedule shall include all workers located in the facility from which the goods and services are produced and shall include the same information for other facilities which have a significant relationship to the performance of work under the contract.

1104.4 If the experience of the contractor with any local union from which it will secure employees indicates that the union will not refer sufficient minorities or women to meet minority or female employment commitments, the contractor shall, not less than ten (10) days prior to the employment of any person on the project subject to the jurisdiction of that local union, do the following:

(a) Notify the District of Columbia Department of Employment Services and at least two (2) minority and two (2) female referral organizations of the contractor's personnel needs, and request referral of minority and female workers; and

(b) Notify any minority and female workers who have been listed with the contractors as awaiting vacancies.

1104.5 If, within five (5) working days prior to commencement of work, the contractor determines that the Department of Employment Services or the minority or female referral organizations are unable to refer sufficient minorities or women to meet its commitments, the contractor may take steps to hire, by referral or otherwise, from the local union membership to fill the remaining job openings, provided that it notifies the local union of its personnel needs and of its employment commitments. Evidence of the notification shall be provided to the Contracting Agency.

1104.6 The contractor shall have standing requests for additional referrals of minority and female workers with the local union, the Department of Employment Services, and the other referral sources, until such time as the contractor has met its minority and female employment commitments.

1104.7 If the contractor desires to lay off some of its employees in a given trade on a construction site, it shall ensure that the required number of minority and female employees remain on the site to meet the minority and female commitments.

1104.8 No contractor shall refuse employment to any individual who has minimal facility to speak English except where the contractor can demonstrate that the facility to speak English is necessary for the performance of the job.

1104.9 No union with which the contractor has a collective bargaining agreement shall refuse to refer minority and female employees to such contractor.

1104.10 To the extent that contractors have delegated the responsibility for some of their employment practices to some other organization or agency which prevents them from meeting their equal opportunity obligations, those contractors shall not be considered to be in compliance with this chapter.

1104.11 The obligations of the contractor shall not be reduced, modified, or subject to any provision in any collective bargaining agreement with labor organization which provides that the labor organizations shall have the exclusive or primary opportunity to refer employees.

1104.12 When any contractor employs a minority person or woman in order to comply with this chapter, those persons shall be advised of their right to seek union membership, the contractor shall provide whatever assistance may be appropriate to enable that person to obtain membership, and the contractor shall notify the appropriate union of that person's employment.

1104.13 The contractor shall not discharge, refuse to employ, or otherwise adversely affect any minority person or woman because of any provision in any collective bargaining agreement, or any understanding, written or oral that the contractor may have with any labor organization.

1104.14 If at any time, because of lack of cooperation or overt conduct, a labor organization impedes or interferes with the contractor's Affirmative Action Program, the contractor shall notify the Contracting Agency and the Director immediately, setting forth the relevant circumstances.

1104.15 In any proceeding involving a disagreement between a labor organization and the contractor over the implementation of the contractor's Affirmative Action Program, the Contracting Agency and the Office of Human Rights may become a party to the proceeding.

1104.16 In determining whether or not a contractor is utilizing minorities and females pursuant to Section 1108, consideration shall be given to the following factors:

(a) The proportion of minorities and women employed in the trades and as laborers in the construction industry within the District of Columbia;

(b) The proportion of minorities and women employed in the crafts or as operatives in non-construction industries with in the District of Columbia;

(c) The number and ratio of unemployed minorities and women to total unemployment in the District of Columbia;

(d) The availability of qualified and qualifiable minorities and women for employment in any comparable line of work, including where they are now working and how they may be brought into the contractor's workforce;

(e) The effectiveness of existing training programs in the area, including the number who complete training, the length and extent of training, employer experience with trainees, and the need for additional or expanded training programs; and

(f) The number of additional workers that could be absorbed into each trade or line of work without displacing present employees, including consideration of present employee shortages, projected growth of the trade or line of work, and projected employee turnover.

1104.17 The contractor's commitment to specific standards for the utilization of minorities and females as required under this chapter shall include a commitment to make every good faith effort to meet

those standards. If the contractor has failed to meet the standards, a determination of "good faith" shall be based upon the contractor's documented equal opportunity efforts to broaden its equal employment program which shall include, but may not necessarily be limited to, the following requirements:

(a) The contractor shall notify the community organizations that the contractor has employment opportunities available and shall maintain records of the organizations' responses;

(b) The contractor shall maintain a file of the names and addresses of each minority and female worker referred to it and what action was taken with respect to each referred worker. If that worker was not sent to the union hiring hall for referral or if the worker was not employed by the contractor, the contractor's file shall be documented and the reasons therefore;

(c) The contractor shall notify the Contracting Agency and the Director when the union or unions with which the contractor has a collective bargaining agreement has not referred to the contractor a minority or female worker originally sent to the union by the contractor for union registration, or the contractor has other information that the union referral process has impeded the contractor's efforts to meet its goals;

(d) The contractor shall participate in training programs related to its personnel needs;

(e) The contractor shall disseminate its EEO policy internally by doing the following:

(1) Including it in any organizational manual;

(2) Publicizing it in company newspapers, annual report, etc.;

(3) Conducting staff, employee, and union representatives meetings to explain and discuss the policy;

(4) Posting; and

(5) Reviewing the policy with minority and female employees.

(f) The contractor shall disseminate its EEO policy externally by doing the following:

(1) Informing and discussing it with all recruitment sources;

(2) Advertising in news media, specifically including news media directed to minorities and women;

(3) Notifying and discussing it with all known minority and women's organizations; and

(4) Notifying and discussing it with all subcontractors and suppliers.

1104.18 The contractor shall make specific recruitment efforts, both written and oral, directed at all minority and women's training organizations within the contractor's recruitment area.

1104.19 The contractor shall encourage present employees to assist in the recruitment of minorities and women for employment.

1104.20 The contractor shall validate all qualifications, selection requirements, and tests in accordance with the guidelines of the Equal Employment Opportunity Commission.

1104.21 The contractor shall make good faith efforts to provide after school, summer and vacation employment to minority youths and young women.

1104.22 The contractor shall develop on-the-job training opportunities, and participate and assist in any association or employer group training programs relevant to the contractor' s employee needs.

1104.23 The contractor shall continually inventory and evaluate all minority and female personnel for promotion opportunities.

1104.24 The contractor shall make sure that seniority practices, job classifications, qualifications, etc. do not have a discriminatory effect on minorities and women.

1104.25 The contractor shall make certain that all facilities and company activities are nonsegregated.

1104.26 The contractor shall continually monitor all personnel activities to ensure that its EEO policy is being carried out.

1104.27 The contractor may utilize minority banking facilities as depositories for funds which may be involved, directly or indirectly, in the performance of the contract.

1104.28 The contractor shall employ minority and female workers without respect to union membership in sufficient numbers to meet the minority and female employment standards, if the experience of the contractor with any labor union from which it will secure employees does not indicate that it will refer sufficient minorities and females to meet its minority and female employment standards.

1104.29 The contractor shall ensure that all of its employees as well as those of its subcontractors are made knowledgeable about the contractor' s equal opportunity policy.

1104.30 [Reserved]

1104.31 Each contractor shall include in all bid invitations or other pre-bid communications, written or otherwise, with respect to prospective subcontractors, the standards, as applicable, which are required under this chapter.

1104.32 Whenever a contractor subcontracts a portion of the work in any trade, craft or skill it shall include in the subcontract, its commitment made under this chapter, as applicable, which shall be adopted by its subcontractors who shall be bound thereby and by the regulations of this chapter to the full extent as if it were the prime contractor.

1104.33 The prime contractor shall give notice to the Director and the Contracting Agency of any refusal or failure of any subcontractor to fulfill its obligations under this chapter.

1104.34 Failure of compliance by any subcontractor shall be treated in the same manner as a failure by the prime contractor.

1105 EXEMPTIONS

1105.1 Prospective construction contractors shall be exempt from submitting Affirmative Action Programs for contracts amounting to less than twenty-five thousand dollars ($25,000); provided, that when a construction contractor accumulates contracts amounting to twenty-five thousand dollars ($25,000) or more within a period of twelve (12) months that contractor shall be required to submit an Affirmative Action Program for each contract executed thereafter.

1105.2 Prospective non-construction contractors shall be exempt from submitting Affirmative Action Programs for contracts amounting to less than ten thousand dollars ($10,000); provided, that when

a non-construction contractor accumulates contracts amounting to ten thousand dollars ($10,00) or more during a period of twelve (12) months that contractor shall be required to submit an Affirmative Action Program for each contract executed thereafter.

1106 NONRESPONSIBLE CONTRACTORS

1106.1 If a bidder or offeror fails either to submit a complete and satisfactory Affirmative Action Program or to submit a revised Affirmative Action Program that meets the approval of the Director, as required pursuant to this chapter, the Director may direct the Contracting Officer to declare the bidder or offeror to be nonresponsible and ineligible for award of the contract.

1106.2 Any untimely submission of an Affirmative Action Program may, upon order of the Director, be rejected by the Contracting Officer.

1106.3 In no case shall there be any negotiation over the provision of specific utilization standards submitted by the bidder or offeror after the opening of bids or receipt of offer and prior to award.

1106.4 If any directive or order relating to nonresponsibility is issued under this section, the Director shall afford the bidder or offeror a reasonable opportunity to be heard in opposition to such action in accordance with subsection 1118.1, or in support of a request for waiver under section 1109.

1107 NOTICE OF COMPLIANCE

1107.1 Each Contracting Agency shall include, or require the contract bidder or offeror to include, in the invitation for bids or other solicitation used for a D.C. Government-involved contract, a notice stating that to be eligible for consideration, each bidder or offeror shall be required to comply with the provisions of this chapter for the trades, crafts and skills to be used during the term of the performance of the contract whether or not the work is subcontracted.

1108 MINIMUM STANDARDS FOR MINORITY AND FEMALE EMPLOYMENT

1108.1 The minimum standards for the utilization of minorities in the District of Columbia Government construction contracts shall be forty-two percent (42%) in each trade for each project, and an aggregate workforce standard of six and nine-tenths percent (6.9%) for females in each project. Any changes in Federal standards pertaining to minority group and female employment in Federally-involved construction contracts shall be taken into consideration in any review of these requirements.

1108.2 The construction contractor' s standards established in accordance with subsection 1108.1 shall express the contractor' s commitment of the forty-two percent (42%) of minority personnel who will be working in each specified trade on each of the contractor' s District of Columbia Government projects, and the aggregate standard of six and nine-tenths percent (6.9%) for the employment of females in each District of Columbia Government contract.

1108.3 The hours for minority and female workers shall be substantially uniform throughout the entire length of the construction contract for each trade used, to the effect that the same percentage of minority workers in the trades used shall be working throughout the length of work in each trade on each project, and the aggregate percentage in each project for females.

1108.4 The minimum standard for the utilization of minorities in non-construction contracts shall be twenty-five percent (25%) in each of the following nine (9) job categories:

(a) Officials and managers;

(b) Professionals;

(c) Technicians;

(d) Sales workers;

(e) Office and clerical workers;

(f) Craftpersons (Skilled);

(g) Operative (Semi-skilled);

(h) Laborers (Unskilled); and

(i) Service workers.

1108.5 With respect to non-construction contracts the contractor' s standards established in accordance with subsection 1108.4 shall express the contractor' s commitment of the twenty-five percent (25%) of minority personnel who will be working in each specified craft or skill in each contract.

1109 WAIVERS

1109.1 The Director may grant a waiver to a prospective contractor from the requirement to submit a set of minimum standards for the employment of minorities and women in a particular contract, if before the execution of the contract and approval of the Affirmative Action Program, the contractor can document and otherwise prove it is unable to meet the standards in the performance of the contract.

1110 SOLICITATION OF CONTRACT

1110.1 Each solicitation for contract covered by section 1104 shall contain a statement that contractors shall comply with the minimum standards established pursuant to these rules for ensuring equal opportunity.

1110.2 The contract solicitation shall require that each bidder or offeror certify that it intends to meet the applicable minimum standards in section 1108 in order to be considered for the contract.

1111 PRIOR TO EXECUTION OF CONTRACT

1111.1 Upon being designated the apparent low bidder or offeror, that contractor shall submit a detailed Affirmative Action Program that sets forth the following:

(1) The composition of its current total workforce; and

(2) The composition of the workforce by race, color, national origin, and sex to be used in the performance of the contract and that of all known subcontractors that will be utilized to perform the contract.

1111.2 The apparent low bidder or offeror shall submit an Affirmative Action Program in accordance with section 1104 describing the actions it will take to ensure compliance with this chapter which shall be subject, prior to the execution of any contract, to the approval of the Director.

1111.3 If the Office of Human Rights does not act within ten (10) working days after the receipt of the Affirmative Action Program sent for approval, the Contracting Agency may proceed on its own determination to execute the contract.

1111.4 The apparent low bidder or offeror shall submit an Affirmative Action Program within a period of time to specified by each Contracting Agency, but which shall not exceed ten (10) working days after becoming the apparent contractor.

1111.5 The apparent low bidder or offeror shall furnish all information and reports to the Contracting Agency as required by this chapter, and shall permit access to all books or records pertaining to its employment practices or worksites.

1111.6 No contract subject to section 1104 shall be executed by the Contracting Agency, if the apparent low bidder or offeror does not submit an Affirmative Action Program, or if the Program has been disapproved in writing by the Director.

1111.7 If there is disagreement between the contractor and the Contracting Officer as to the adequacy of the Affirmative Action Program, the matter shall be referred to the Director for a decision.

1112 AFTER EXECUTION OF CONTRACT

1112.1 Each contractor shall maintain throughout the term of the contract the minimum standards for the employment of minorities and women, as set forth in the approved Affirmative Action Program.

1112.2 Each contractor shall require that each subcontractor, or vendor under the contract comply with the provision of the contract and the Affirmative Action Program.

1112.3 Each contractor shall furnish all information as required by this chapter, and permit access to all books and records pertaining to the contractor' s employment practices and work sites by the Director and the Contracting Agency for purposes of investigation to ascertain compliance with this chapter.

1113 MONITORING AND EVALUATION

1113.1 The Director shall, from time to time, monitor and evaluate all District of Columbia Government agencies, including those independent agencies and commissions not required to submit the Affirmative Action Program of their contractors, to ensure compliance with the equal opportunity obligations in contracts, as provided for in this chapter.

1114 AFFIRMATIVE ACTION TRAINING PROGRAM

1114.1 Each contractor, in fulfilling its affirmative action responsibilities under a contract with the District of Columbia Government, shall be required to have, as part of its Affirmative Action Program, an existing training program for the purpose of training, upgrading, and promotion of minority and female employees or to utilize existing programs. Those programs shall include, but not be limited to, the following:

(a) To be consistent with its personnel requirements, the contractor shall make full use of the applicable training programs, including apprenticeship, on-the job training, and skill refinement training for journeymen. Recruitment for the program shall be designed to provide for appropriate participation by minority group members and women;

(b) The contractor may utilize a company-operated skill refinement training program. This program shall be formal and shall be responsive to the work to be performed under the contract;

(c) The contractor may utilize formal private training institutions that have as their objective training and skill refinement appropriate to the classification of the workers employed. When training is provided by a private organization the following information shall be supplied:

(1) The name of the organization;

(2) The name, address, social security number, and classification of the initial employees and any subsequent employees chosen during the course of the course of the contract; and

(3) The identity of the trades, and crafts or skills involved in the training.

1114.2 If the contractor relies, in whole or in part, upon unions as a source of its workforce, the contractor shall use its best efforts, in cooperation with unions, to develop joint training programs aimed toward qualifying more minorities and females for membership in the union, and increasing the skills of minority and female employees so that they may qualify for higher paying employment.

1114.3 Approval of training programs by the Contracting Agency shall be predicated, among other things, upon the quality of training, numbers of trainees and trades, crafts or skills involved, and whether the training is responsive to the policies of the District of Columbia and the needs of the minority and female community. Minority and female applicants for apprenticeship or training should be selected in sufficient numbers as to ensure an acceptable level of participation sufficient to overcome the effects of past discrimination.

1115 COMPLIANCE REVIEW

1115.1 The Director and the Contracting Agency shall review the contractor's employment practices during the performance of the Contract. Routine or special reviews of contractors shall be conducted by the Contracting Agency or the Director in order to ascertain the extent to which the policy of Mayor's Order No. 85-85, and the requirements in this chapter are being implemented and to furnish information that may be useful to the Director and the Contracting Agency in carrying out their functions under this chapter.

1115.2 A routine compliance review shall consist of a general review of the practices of the contractor to ascertain compliance with the requirements of this chapter, and shall be considered a normal part of contract administration.

1115.3 A special compliance review shall consist of a comprehensive review of the employment practices of the contractor with respect to the requirements of this chapter, and shall be conducted when warranted.

1116 ENFORCEMENT

1116.1 If the contractor does not comply with the equal opportunity clauses in a particular contract, including subsections 1103.2 through 1103.10 of this chapter, that contract may be cancelled in whole or in part, and the contractor may be declared by the Director or the Contracting Officer to be ineligible for further District of Columbia Government Contracts subject to applicable laws and regulations governing debarment.

1116.2 If the contractor meets its goals or if the contractor can demonstrate that it has made every good faith effort to meet those goals, the contractor will be presumed to be in compliance with this chapter, and no formal sanction shall be instituted unless the Director otherwise determines that the contractor is not providing equal employment opportunity.

1116.3 When the Director proceeds with a formal hearing she or he has the burden of proving that the contractor has not met the requirements of this chapter, but the contractor's failure to meet its goals shall shift to it the requirement to come forward with evidence to show that it has met the good faith requirements of this chapter.

1117 COMPLAINTS

1117.1 The Director may initiate investigations of individual instances and patterns of discriminatory conduct, initiate complaints thereupon and keep the Contracting Agency informed of those actions.

1117.2 If the investigation indicates the existence of an apparent violation of the non-discrimination provisions of the contract required under section 1103 of this chapter the matter may be resolved by the methods of conference, conciliation, mediation, or persuasion.

1117.3 If an apparent violation of the non-discrimination provisions of the contract required under section 1103 of this chapter is not resolved by methods of conference, conciliation, mediation, or persuasion, the Director of the Contracting Officer may issue a notice requiring the contractor in question to show cause, within thirty (30) days, why enforcement proceedings or other appropriate action should not be initiated.

1117.4 Any employee of any District of Columbia Government contractor or applicant for employment who believes himself or herself to be aggrieved may, in person or by an authorized representative, file in writing, a complaint of alleged discrimination with the Director.

1118 HEARINGS

1118.1 In the event that a dispute arises between a bidder, offeror or prospective contractor and the Director or the Contracting Officer as to whether the proposed program of affirmative action for providing equal employment opportunity submitting by such bidder, offeror or prospective contractor complies with the requirements of this chapter and cannot be resolved by the methods of conference, conciliation, mediation, or persuasion, the bidder, offeror or prospective contractor in question shall be afforded the opportunity for a hearing before the Director.

1118.2 If a case in which an investigation by the Director or the Contracting Agency has shown the existence of an apparent violation of the non-discrimination provisions of the contract required under section 1103 is not resolved by the methods specified in subsection 1117.2, the Director may issue a notice requiring the contractor in question to show cause, within thirty (30) days, why enforcement proceedings or other appropriate action should not be initiated. The contractor in question shall also be afforded the opportunity for a hearing before the Director.

1118.3 The Director may hold a hearing on any compliant or violation under this chapter, and make determinations based on the facts brought before the hearing.

1118.4 Whenever the Director holds a hearing it is to be held pursuant to the Human Rights Act of 1977, a notice of thirty (30) working days for the hearing shall be given by registered mail, return receipt requested, to the contractor in question. The notice shall include the following:

(a) A convenient time and place of hearing;

(b) A statement of the provisions in this chapter or any other laws or regulations pursuant to which the hearing is to be held; and

(c) A concise statement of the matters to be brought before the hearing.

1118.5 All hearings shall be open to the public and shall be conducted in accordance with rules, regulations, and procedures promulgated pursuant to the Human Rights Act of 1977.

1119 SANCTIONS

1119.1 The Director, upon finding that a contractor has failed to comply with the non-discrimination provisions of the contract required under section 1103, or has failed to make a good faith effort to achieve the utilization standards under an approved Affirmative Action Program, may impose sanctions contained in this section in addition to any sanction or remedies as may be imposed or invoked under the Human Rights Act of 1977.

1119.2 Sanctions imposed by the Director may include the following:

(a) Order that the contractor be declared ineligible from consideration for award of District of Columbia Government contracts or subcontracts until such time as the Director may be satisfied that the contractor has established and will maintain equal opportunity policies in compliance with this chapter; and

(b) Direct each Contracting Officer administering any existing contract to cancel, terminate, or suspend the contract or any portion thereof, and to deny any extension, modification, or change, unless the contractor provides a program of future compliance satisfactory to the Director.

1119.3 Any sanction imposed under this chapter may be rescinded or modified upon reconsideration by the Director.

1119.4 An appeal of any sanction imposed by order of the Director under this chapter may be taken pursuant to applicable clauses of the affected contract or provisions of law and regulations governing District of Columbia Government contracts.

1120 NOTIFICATIONS

1120.1 The Director shall forward in writing notice of his or her findings of any violations of this chapter to the Contracting Officer for appropriate action under the contract.

1120.2 Whenever it appears that the holder of or an applicant for a permit, license or franchise issued by any agency or authority of the Government of the District of Columbia is a person determined to be in violation of this chapter the Director may, at any time he or she deems that action the Director may take or may have taken under the authority of this chapter, refer to the proper licensing agency or authority the facts and identities of all persons involved in the violation for such action as the agency or authority, in its judgement, considers appropriate based upon the facts thus disclosed to it.

1120.3 The Director may publish, or cause to be published, the names of contractors or unions which have been determined to have complied or have failed to comply with the provisions of the rules in this chapter.

1121 DISTRICT ASSISTED PROGRAMS

1121.1 Each agency which administers a program involving leasing of District of Columbia Government owned or controlled real property, or the financing of construction under industrial revenue bonds or urban development action grants, shall require as a condition for the approval of any agreement for leasing, bond issuance, or development action grant, that the applicant undertake and agree to incorporate, or cause to be incorporated into all construction contracts relating to or assisted by such agreements, the contract provisions prescribed for District of Columbia Government contracts by section 1103, preserving in substance the contractor's obligation under those provision.

1199 DEFINITIONS

1199.1 The following words and phrases set forth in this section, when used in this chapter, shall have the following meanings ascribed:

Contract – any binding legal relationship between the District of Columbia and a contractor for supplies or services, including but not limited to any District of Columbia Government or District of Columbia Government assisted construction or project, lease agreements, Industrial Revenue Bond financing, and Urban Development Action grant, or for the lease of District of Columbia property in which the parties, respectively, do not stand in the relationship of employer and employee.

Contracting Agency – any department, agency, or establishment of the District of Columbia which is authorized to enter into contracts.

Contracting Officer – any official of a contracting agency who is vested with the authority to execute contracts on behalf of said agency.

Contractor – any prime contractor holding a contract with the District of Columbia Govemment. The term shall also refer to subcontractors when the context so indicates.

Director – the Director of the Office of Human Rights, or his or her designee.

Dispute – any protest received from a bidder or prospective contractor relating to the effectiveness of his or her proposed program of affirmative action for providing equal opportunity.

Minority – Black Americans, Native Americans, Asian Americans, Pacific Islander Americans, and Hispanic Americans. In accordance with D.C. Code, Section 1-1142(1) (Supp. 1985).

Subcontract – any agreement made or executed by a prime contractor or a subcontractor where a material part of the supplies or services, including construction, covered by an agreement is being obtained for us in the performance of a contract subject to Mayor' s Order No. 85-85, and any rules, regulations, and procedures issued pursuant thereto.

Subcontractor – any contractor holding a contract with a District prime contractor calling for supplies or services, including construction, required for the performance of a contract subject to Mayor' s Order No. 85-85, and any rules, regulations, and procedures promulgated pursuant thereto.

FIRST SOURCE EMPLOYMENT AGREEMENT

Contract Number: _____

Contract Amount: _____

Project Name: _____

Project Address: _____ Ward:_____

Nonprofit Organization with 50 Employees or Less: (Yes) ____ (No) ____

This First Source Employment Agreement, in accordance with D. C. Law 14-24, D.C. Law 5-93, and Mayor's Order 83-265 for recruitment, referral, and placement of District of Columbia residents, is between the District of Columbia Department of Employment Services, hereinafter referred to as DOES, and _____, hereinafter, referred to as EMPLOYER. Under this Employment Agreement, the EMPLOYER will use DOES as its first source for recruitment, referral, and placement of new hires or employees for the new jobs created by this project and will hire 51% District of Columbia residents for all new jobs created, as well, as 51% of apprentices employed in connection with the project shall be District residents registered in programs approved by the District of Columbia Apprenticeship Council.

I. GENERAL TERMS

A. The EMPLOYER will use DOES as its first source for the recruitment, referral and placement of employees.

B. The EMPLOYER shall require all contractors and subcontractors, with contracts totaling $100,000 or more, to enter into a First Source Employment Agreement with DOES.

C. DOES will provide recruitment, referral and placement services to the EMPLOYER subject to the limitations set out in this Agreement.

D. DOES participation in this Agreement will be carried out by the Office of the Director, with the Office of Employer Services, which is responsible for referral and placement of employees, or such other offices or divisions designated by DOES.

E. This Agreement shall take effect when signed by the parties below and shall be fully effective for the duration of the contract and any extensions or modifications to the contract.

F. This Agreement shall not be construed as an approval of the EMPLOYER'S bid package, bond application, lease agreement, zoning application, loan, or contract/subcontract.

G. DOES and the EMPLOYER agree that for purposes of this Agreement, new hires and jobs created (both union and nonunion) include all EMPLOYER'S job openings and vacancies in the Washington Standard Metropolitan Statistical Area created as a result of internal promotions, terminations, and expansions of the EMPLOYER'S workforce, as a result of this project, including loans, lease agreements, zoning applications, bonds, bids, and contracts.

H. For purposes of this Agreement, apprentices as defined in D.C. Law 2-156, as amended, are included.

I. The EMPLOYER shall register an apprenticeship program with the D.C. Apprenticeship Council for construction or renovation contracts or subcontracts totaling $500,000 or more. This includes any construction or renovation contract or subcontract signed as the result of, but is not limited to, a loan, bond, grant, Exclusive Right Agreement, street or alley closing, or a leasing agreement of real property for one (1) year or more.

J. All contractors who contract with the Government of the District of Columbia to perform information technology work with a single contract or cumulative contracts of at least $500,000, let within any twelve (12) month period shall be required to register an apprenticeship program with the District of Columbia Apprenticeship Council.

K. The term "information technology work" shall include, but is not limited to, the occupations of computer programmer, programmer analyst, desktop specialist, technical support specialist, database specialist, network support specialist, and any other related occupations as the District of Columbia Apprenticeship Council may designate by regulation.

II. RECRUITMENT

A. The EMPLOYER will complete the attached Employment Plan, which will indicate the number of new jobs projected, salary range, hiring dates, and union requirements. The EMPLOYER will notify DOES of its specific need for new employees as soon as that need is identified.

B. Notification of specific needs, as set forth in Section II.A. must be given to DOES at least five (5) business days (Monday - Friday) before using any other referral source, and shall include, at a minimum, the number of employees needed by job title, qualification, hiring date, rate of pay, hours of work, duration of employment, and work to be performed.

C. Job openings to be filled by internal promotion from the EMPLOYER'S current workforce need not be referred to DOES for placement and referral.

D. The EMPLOYER will submit to DOES, prior to starting work on the project, the names, and social security numbers of all current employees, including apprentices, trainees, and laid-off workers who will be employed on the project.

III. REFERRAL

DOES will screen and refer applicants according to the qualifications supplied by the EMPLOYER.

IV. PLACEMENT

A. DOES will notify the EMPLOYER, prior to the anticipated hiring dates, of the number of applicants DOES will refer. DOES will make every reasonable effort to refer at least two qualified applicants for each job opening.

B. The EMPLOYER will make all decisions on hiring new employees but will in good faith use reasonable efforts to select its new hires or employees from among the qualified persons referred by DOES.

C. In the event DOES is unable to refer the qualified personnel requested, within five (5) business days (Monday - Friday) from the date of notification, the EMPLOYER will be free to directly fill remaining positions for which no qualified applicants have been referred. Notwithstanding, the EMPLOYER will still be required to hire 51% District residents for the new jobs created by the project.

D. After the EMPLOYER has selected its employees, DOES will not be responsible for the employees' actions and the EMPLOYER hereby releases DOES, and the Government of the District of Columbia, the District of Columbia Municipal Corporation, and the officers and employees of the District of Columbia from any liability for employees' actions.

V. TRAINING

DOES and the EMPLOYER may agree to develop skills training and on-the-job training programs; the training specifications and cost for such training will be mutually agreed upon by the EMPLOYER and DOES and set forth in a separate Training Agreement.

VI. CONTROLLING REGULATIONS AND LAWS

A. To the extent this Agreement is in conflict with any labor laws or governmental regulations, the laws or regulations shall prevail.

B. DOES will make every effort to work within the terms of all collective bargaining agreements to which the EMPLOYER is a party.

C. The EMPLOYER will provide DOES with written documentation that the EMPLOYER has provided the representative of any involved collective bargaining unit with a copy of this Agreement and has requested comments or objections. If the representative has any comments or objections, the EMPLOYER will promptly provide them to DOES.

VII. EXEMPTIONS

A. Contracts, subcontracts or other forms of government-assistance less than $100,000.

B. Employment openings the contractor will fill with individuals already employed by the company.

C. Job openings to be filled by laid-off workers according to formally established recall procedures and rosters.

D. Suppliers located outside of the Washington Standard Metropolitan Statistical Area and who will perform no work in the Washington Standard Metropolitan Statistical Area.

VIII. AGREEMENT MODIFICATIONS, RENEWAL, MONITORING, AND PENALTIES

A. If, during the term of this Agreement, the EMPLOYER should transfer possession of all or a portion of its business concerns affected by this Agreement to any other party by lease, sale, assignment, merger, or otherwise, the EMPLOYER as a condition of transfer shall:

1. Notify the party taking possession of the existence of the EMPLOYER'S Agreement.

2. Notify the party taking possession that full compliance with this Agreement is required in order to avoid termination of the project.

3. EMPLOYER shall, additionally, advise DOES within seven (7) business/calendar days of the transfer. This advice will include the name of the party taking possession and the name and telephone of that party's representative.

B. DOES shall monitor EMPLOYER'S performance under this Agreement. The EMPLOYER will cooperate in DOES' monitoring effort and will submit a Contract Compliance Form to DOES monthly.

C. To assist DOES in the conduct of the monitoring review, the EMPLOYER will make available payroll and employment records for the review period indicated.

D. If additional information is needed during the review, the EMPLOYER will provide the requested information to DOES.

E. With the submission of the final request for payment from the District, the EMPLOYER shall:

1. Document in a report to the Contracting Officer its compliance with the requirement that 51% of the new employees hired by the project be District residents; or

2. Submit a request to the Contracting Officer for a waiver of compliance with the requirement that 51% of the new employees hired by the project be District residents and include the following documentations:
   a. Material supporting a good faith effort to comply;
   b. Referrals provided by DOES and other referral sources; and
   c. Advertisement of job openings listed with DOES and other referral sources.

F. The Contracting Officer may waive the requirement that 51% of the new employees hired by the project be District residents, if the Contracting Officer finds that:

1. A good faith effort to comply is demonstrated by the contractor;

2. The EMPLOYER is located outside the Washington Standard Metropolitan Statistical Area and none of the contract work is performed inside the Washington Standard Metropolitan Statistical Area;

   The Washington Standard Metropolitan Statistical Area includes the District of Columbia, the Virginia Cities of Alexandria, Falls Church, Manasas, Manasas Park, Fairfax, and Fredericksburg; the Virginia Counties of Fairfax, Arlington, Prince William, Loundon, Stafford, Clarke, Warren, Fauquier, Culpeper, Spotsylvania, and King George; the Maryland Counties of Montgomery, Prince Georges, Charles, Frederick, and Calvert; and the West Virginia Counties of Berkeley and Jefferson.

3. The EMPLOYER enters into a special workforce development training or placement arrangement with DOES; or

4. DOES certifies that insufficient numbers of District residents in the labor market possess the skills required by the positions created as a result of the contract.

G. Willful breach of the First Source Employment Agreement by the EMPLOYER, or failure to submit the Contract Compliance Report, or deliberate submission of falsified data, may be enforced by the Contracting Officer through imposition of penalties, including monetary fines of 5% of the total amount of the direct and indirect labor costs of the contract.

H Nonprofit organizations with 50 or less employees are exempted from the requirement that 51% of the new employees hired on the project be District residents.

I. The EMPLOYER and DOES, or such other agent as DOES may designate, may mutually agree to modify this Agreement.

J. The project may be terminated because of the EMPLOYER'S non-compliance with the provisions of this Agreement.

IX. Is your firm a certified Local, Small, Disadvantaged Business Enterprise (LSDBE)?
YES NO
If yes, certification number:_____

X. Do you have a registered Apprenticeship program with the D.C. Apprenticeship Council?
YES NO
If yes, D.C. Apprenticeship Council Registration Number: _____

XI. Indicate whether your firm is a subcontractor on this project: YES NO
If yes, name of prime contractor: _____

Dated this_____day of_____20_____

_____ _____
Signature Dept. of Employment Services Signature of Employer

_____
Name of Company

_____
Address

_____
Telephone

_____
E-mail

EMPLOYMENT PLAN

NAME OF FIRM_____

ADDRESS_____

TELEPHONE NUMBER_____FEDERAL IDENTIFICATION NO._____

CONTACT PERSON_____TITLE_____

E-mail:_____ TYPE OF BUSINESS: _____

ORIGINATING DISTRICT AGENCY_____

CONTRACTING OFFICER: _____ TELEPHONE NUMBER: _____

TYPE OF PROJECT_____FUNDING AMOUNT_____

PROJECTED START DATE_____PROJECT DURATION_____

NEW JOB CREATION PROJECTIONS (Attach additional sheets, as needed.) Please indicate the new position(s) your firm will create as a result of this project.

	JOB TITLE	# OF JOBS F/T P/T	SALARY RANGE	UNION MEMBERSHIP REQUIRED NAME LOCAL#	PROJECTED HIRE DATE
A					
B					
C					
D					
E					
F					
G					
H					
I					
J					
K					

CURRENT EMPLOYEES: Please list the names and social security numbers of all current employees including apprentices and trainees who will be employed on the project. Attach additional sheets as needed.

NAME OF EMPLOYEE	SOCIAL SECURITY NUMBER or EMPLOYEE IDENTIFICATION NUMBER

WORKING COPY OF SETTLEMENT ORDER OF JANUARY 25, 1999,
INCLUDING ALL AMENDMENTS THROUGH JULY 30, 2001

Prepared by Plaintiffs= Counsel

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

OSCAR SALAZAR, *et al*., on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	
v.	)	Civil Action No. 93-452 (GK)
	)	*In Forma Pauperis*
THE DISTRICT OF COLUMBIA, *et al*.,	)	
Defendants.	)	

ORDER MODIFYING THE AMENDED REMEDIAL ORDER OF MAY 6, 1997
AND VACATING THE ORDER OF MARCH 27, 1997

WHEREAS, the parties desire to resolve the pending appeals in this case,

WHEREAS, upon consideration of Plaintiffs' motion for entry of this Order Modifying the Amended Remedial Order of May 6, 1997, and Vacating the Order of March 27, 1997 (hereafter "Order"), and Defendants' response agreeing to the motion, the Court concludes that the modifications to the Amended Remedial Order of May 6, 1997, and the vacation of the Order of March 27, 1997, set forth herein are fair, reasonable and adequate,

IT IS, this ____22nd_____ day of ____January_____, 199~~8~~9, ORDERED, ADJUDGED AND DECREED AS FOLLOWS:

WORKING COPY OF SETTLEMENT ORDER OF JANUARY 25, 1999,
INCLUDING ALL AMENDMENTS THROUGH JULY 30, 2001

Prepared by Plaintiffs= Counsel

1. The Amended Remedial Order of May 6, 1997, and the Order of March 27, 1997, are vacated.

I. Monitor

2. Thomas W. Chapman, M.P.H., FACHE, served as Monitor pursuant to Orders of the Court from March 10, 1997, to June 16, 1998. The parties understand that the Court is in the process of selecting a new Monitor. The Monitor shall have the duties and responsibilities set forth in this Order.

3. The function of the Monitor is to report, record, evaluate, observe, and provide recommendations, as appropriate, about Defendants= activities so as to achieve full compliance with the provisions of this Order. The Monitor shall remain neutral and objective in carrying out all monitoring duties. The Monitor shall receive reasonable compensation from the District of Columbia, as determined by the Court.

4. The Monitor shall be under the direct supervision and control of the Court, and shall not be empowered to direct Defendants to take or refrain from taking any specific action to achieve compliance with the provisions of this Order. The Monitor shall endeavor to work cooperatively with Defendants and Plaintiffs, and may recommend efficient and economical methods by which Defendants may achieve compliance.

5. From time to time, as directed by the Court or as provided in this Order, the Monitor shall prepare written reports to the Court, copies to counsel, indicating the status of Defendants= compliance with said Order, and the factors that affect such compliance. The parties shall have thirty (30) days

thereafter within which to submit comments on such reports, and prior to the Court taking any action, unless otherwise stated in this Order or directed by the Court.

II. Processing of Medicaid Applications (Claim 4)

6. (a) With respect to non-disability, non-foster care, non-Public Assistance Medicaid applications (hereafter, "application" or "applicant"), Defendants shall determine eligibility and mail a notice of decision within forty-five (45) days of the date of receipt of all applications.

(b) This paragraph shall apply to all applications including pending applications as of the date of entry of this Order.

(c) Provided, however, if an applicant submits the documentation and/or verification required for the District to determine the applicant's Medicaid eligibility more than 40 days after the receipt of the signed application by the District, the District shall have 5 days to process the application from the time that the applicant submits all the documentation and/or verification. The processing of an application within 5 days of the time the documentation and/or verification is submitted pursuant to this subparagraph shall be considered as timely. The processing of an application later than 5 days after the time the documentation and/or verification is submitted pursuant to this subparagraph shall be considered as untimely. This subparagraph shall only apply if the District has requested from the applicant, in writing, all the documentation and/or verification that is required and has not been submitted (a) within 5 days of the time the application is submitted; or (b) within 5 days of the applicant's submission of information or a document which first causes the need for additional documentation and/or verification.

7. Each member of the plaintiff class has a right to a decision on an application within forty-five (45) days of making the application. This right may be asserted only by individuals invoking their right to a fair hearing.

8. Defendants shall be in compliance with paragraph 6 above, unless, averaged over any four (4) consecutive month period, Defendants fail to issue decisions on at least 95% of all applications within the time period provided in paragraph 6 above.

9. No month shall be considered in determining whether Defendants are in violation of paragraphs 6 and 8 above or in calculating the termination of Section II of this Order under paragraph 74 below in which an event beyond the reasonable control of Defendants causes Defendants to fail to comply with paragraphs 6 and 8. An "event beyond the reasonable control of Defendants" shall include, but not be limited to, a central computer breakdown, an unusually high number of employee resignations or terminations, a significant expansion of Medicaid eligibility criteria (based on changes in federal or District law or policy) such that new classes of persons are eligible, one or more employees having intentionally concealed from Income Maintenance Administration (IMA) management the fact that five (5) or more applications have not been processed, or a reduction in force (RIF) attributable to a substantial reduction in the budget of the Department of Human Services that affects a significant number of supervisors or employees who are necessary to the processing of applications. No event shall satisfy the requirements of this paragraph unless Plaintiffs' counsel is notified in writing of the claim and the justification for the claim (a) within fourteen (14) days of Defendants having actual notice that the event will cause failure to comply with

this paragraph, or (b) within twenty-two (22) days of the end of the reporting month affected by the event, whichever is sooner.

10. (a) Defendants shall have the right to suspend the provisions of paragraphs 6 and 8 during the initial implementation of the State Children's Health Insurance Program (SCHIP). No month during which the provisions of paragraphs 6 and 8 are suspended may be used to justify termination of Section II of this Order under paragraph 74. Defendants may exercise this right for one continuous period at any time during the first twelve (12) months of the implementation of the SCHIP program. This paragraph shall not be applicable unless Defendants notify Plaintiffs within 30 days of the time the SCHIP program begins to be implemented and by the last day of the month as to which Defendants begin the suspension period.

(b) This paragraph discusses the SCHIP program solely with relation to its impact on Defendants' obligation to process Medicaid applications of presently recognized members of the plaintiff class within 45 days of submission. This Order is not intended to address, and does not decide, whether children receiving medical services under the SCHIP program are, or are not, members of any of the plaintiff sub-classes in this litigation. If Plaintiffs believe that applicants for or recipients of services under the SCHIP program are members of one or more of the plaintiff sub-classes, Plaintiffs may file a motion with the Court for a determination of this issue.

11. The 95% and 98% standards in paragraphs 8 above and 12 below shall be calculated each month on the basis of the total number of cases decided (i.e., approved or denied) in the month. The ratio

shall be computed in the following manner: (number of cases decided in accordance with paragraph 6 above or paragraph 12 below) divided by (total number of cases decided in the month). 12.

Any application pending on the 46th day after receipt by Defendants or on the 6th day after the applicant completes submission of all information reasonably requested by Defendants no more than five (5) days after the initial application or within five (5) days of the applicant's submission of information or a document which first causes the need for additional documentation and/or verification, whichever is later, shall receive an eligibility determination on the 46th day, or the 6th day, whichever is applicable. If an application is denied, Defendants shall inform Plaintiffs of the name and case number and shall state the reason for denial within thirty (30) days of the due date of the report required by paragraph 16 below. Defendants shall not be in violation of this paragraph so long as 98% of the applications receive eligibility determinations by the 60th day. Defendants shall not be in violation of this paragraph in any month in which an event beyond the reasonable control of Defendants causes Defendants to fail to comply with this paragraph. An "event beyond the reasonable control of Defendants" shall include, but not be limited to, a central computer breakdown, an unusually high number of employee resignations or terminations, a significant expansion of Medicaid eligibility criteria (based on changes in federal or District law or policy) such that new classes of persons are eligible, one or more employees having intentionally concealed from IMA management the fact that five (5) or more applications have not been processed, or a reduction in force (RIF) attributable to a substantial reduction in the budget of the Department of Human Services that affects a significant number of supervisors or employees who are necessary to the processing of

applications. In such an event, such a month shall not be considered in determining compliance with this paragraph or the termination of Section II of this Order under paragraph 74 below. No event shall satisfy the requirements of this paragraph unless Plaintiffs' counsel is notified in writing of the claim and the justification for the claim (a) within fourteen (14) days of Defendants having actual notice that the event will cause failure to comply with this paragraph, or (b) within twenty-two (22) days of the end of the reporting month affected by the event, whichever is sooner.

13. In determining compliance under paragraphs 8 and 12 above, the following cases shall not be included:

(a) Spend down cases, meaning cases in which there has been a timely denial because the applicant is over-income for Medicaid and there is subsequent activity in the case relating to Defendants' determination whether the applicant has submitted adequate documentation to qualify for Medicaid under the spend down program. The initial determination on such applications shall be included in the reports required by paragraph 16 below and for determining compliance under paragraphs 8 and 12 above;

(b) Reopened cases where there has been a timely denial of a Medicaid application because of the applicant's failure to submit by the 45th day information or documents requested by Defendants in writing no later than five (5) days after the date of the application and there is subsequent activity in the case relating to whether the information or documents submitted by the applicant after the 45th day are adequate to qualify the applicant for Medicaid. The initial determination on the application and any

subsequent application shall be included in the reports required by paragraph 16 below and for determining compliance under paragraphs 8 and 12 above;

(c) Family members added to an existing case where there has been a timely approval of some members of a household for Medicaid and there is a subsequent addition of one or more additional individuals to the household. The initial determination on the household's application and any subsequent application filed for other members of the household shall be included in the reports required by paragraph 16 below and for determining compliance under paragraphs 8 and 12 above; and

(d) Applicants for long-term care Medicaid who are receiving care in a nursing home or hospital, and for whom a delay in an application decision will not result in the applicant being denied medical services. This subparagraph shall only apply if Defendants have requested that the nursing home and/or hospital in which the applicant is receiving care not seek payment from Medicaid applicants while their Medicaid applications are pending. Defendants' request to nursing homes and hospitals may include a disclaimer by Defendants stating that Defendants do not accept liability for any Medicaid applicant's medical expenses until the application is approved. All other applicants for long-term care Medicaid who are not at the time of their application in a nursing home or hospital shall be included in determining compliance under paragraphs 8 and 12 above.

13A. ***Added by Order of August 8, 2000:*** Defendants shall continue their practice of informing Medicaid applicants in a notice issued 30 days after the application is received by Defendants (A30-day notice@) that particular information and/or documents are missing from the application. The 30-day notice shall continue

to state that unless the missing information and/or documents are received within 15 days, the application will be denied. If either the 30th day after the application is received or the 15th day after the 30-day notice is sent falls on a non-business day, the decision on this application may be delayed one or more days after the 45th day. Applications in which the mailing of a decision notice is delayed beyond 45 days solely because (a) the 30th day after the application is received, or (b) the 15th day after the 30-day notice is sent falls on a non-business day, and the 30-day notice or the decision notice is sent on the next available business day, shall be considered timely in determining compliance under paragraphs 8 and 12 above.

14. Defendants shall include in a document provided at the time the application is made to each applicant (including those who mail in applications or submit them at a location other than a Department of Human Services service center), and in all written notices to applicants identifying information or documentation to be supplied to Defendants, a conspicuous statement that (a) Defendants must approve or disapprove the application within forty-five (45) days, and that (b) if the applicant has not received notice of approval or disapproval by the 45th day, the applicant is to call the social service worker to whom the application was submitted (i.e., the SSA or the SSR) and/or the SSR=s supervisor and request that such a determination be made.

15. Defendants shall include in a document provided at the time the application is made to each applicant (including those who mail in applications or submit them at a location other than a Department of Human Services service center), and in all written notices to applicants identifying information or documentation to be supplied to Defendants, a conspicuous statement that, if the eligibility of the applicant is

not determined within forty-five (45) days of the application, the applicant may obtain free legal assistance concerning the application by contacting Plaintiffs' counsel. This statement shall give the name, address and telephone number of Plaintiffs' counsel. The reasonable time and expenses of Plaintiffs' counsel shall be deemed compensable monitoring of this Order under 42 U.S.C. ' 1988.

16. ***Revised by Order of August 8, 2000:*** Beginning no later than August 15, 2000, and on the 15th day of each month thereafter, Defendants shall submit to the Monitor and Plaintiffs' counsel a monthly report or reports for the previous month for each DHS service center (reporting the Multinational Unit separately as long as it exists), listing in alphabetical order by name, case number, and Medicaid identification number (if any), the date each application was received, the date each application was approved or denied, the date of printing of a notice concerning the approval or denial of the application, the number of days between the date of receipt of the application and the date of printing of a notice concerning the approval or denial of the application, and all applications that were still pending more than forty-five (45) days after the date of application on the last day of the month. In addition, the report shall set forth in composite form the total number of applications received in the month, the number approved in the month, and the number denied in the month.

16A. ***Added by Order of August 8, 2000:*** Compliance with paragraph 6 above shall be computed by counting the number of days between the date of receipt of the application and the date of printing of a notice concerning the approval or denial of the application, plus one business day.

16B. ***Added by Order of August 8, 2000:*** For purposes of determining compliance with the percentages in paragraphs 8 and 12 above, only decisions which are reported to a head of household in a notice will be counted. For example, if the District reports three separate decisions concerning a particular family, but there is only one notice issuance date, the three decisions would count as a single decision.

III. Processing of Medicaid Recertifications (Claim 5)

17. With respect to non-Public Assistance, non-foster care, Medicaid recipients (including the disabled) (hereafter, "recipient"), beginning no later June 1, 1999, Defendants shall not terminate a recipient's eligibility for Medicaid benefits unless Defendants have sent the recipient a recertification form at least fifty-five (55) days prior to the end of the eligibility period, and either: (a) the recipient has not returned the recertification form and Defendants have sent an advance termination notice at least twenty-five (25) days prior to the end of the recipient's eligibility period; or (b) some or all of the information and/or documentation requested by Defendants in writing has not been received by Defendants after the recipient has been given a minimum of ten (10) days to produce the information or documentation requested and Defendants have determined to deny continued eligibility for Medicaid and a notice of termination of benefits has been mailed to the recipient fifteen (15) days prior to the actual termination of benefits; or (c) the recertification form, information and documentation have been received by the last day of the eligibility period and Defendants have determined that the recipient is no longer eligible for Medicaid and a notice of termination of benefits has been mailed to the recipient fifteen (15) days prior to the actual termination of benefits.

18. Each member of the plaintiff class has a right not to have Medicaid benefits terminated without advance notice and an opportunity for a hearing. This right may be asserted only by individuals invoking their right to a fair hearing.

19. Defendants shall be in compliance with paragraph 17 above, unless, averaged over any four (4) consecutive month period, Defendants fail to process at least 95% of all recertifications in accordance with the requirements of paragraph 17.

20. No month(s) shall be considered in determining whether Defendants are in violation of paragraphs 17 and 19 above or in calculating the termination of Section III of this Order under paragraph 75 below in which an event beyond the reasonable control of Defendants causes Defendant to fail to comply with paragraph 17 and 19. An "event beyond the reasonable control of Defendants" shall include, but not be limited to, a central computer breakdown, an unusually high number of employee resignations or terminations, one or more employees having intentionally concealed from IMA management the fact that five (5) or more recertifications have not been processed, or a reduction in force (RIF) attributable to a substantial reduction in the budget of the Department of Human Services that affects a significant number of supervisors or employees who are necessary to the processing of recertifications. No event shall satisfy the requirements of this paragraph unless Plaintiffs' counsel is notified in writing of the claim and the justification for the claim (a) within fourteen (14) days of Defendants having actual notice that the event will cause failure to comply with this paragraph, or (b) within twenty-two (22) days of the end of the reporting month affected by the event, whichever is sooner.

21. The 95% standard in paragraph 19 above shall be calculated each month on the basis of the total number of recertification cases in which a determination was made (i.e., approved or terminated) in the month. The ratio shall be computed in the following manner: (number of cases in which a determination was made after both (1) a timely recertification form has been sent to the recipient and (2) a timely and accurate notice of termination or continued eligibility has been sent) divided by (the total number of cases in which a determination was made in the month).

21A. ***Added by Order of August 8, 2000:*** As used in paragraph 21, the term Aa timely and accurate notice of * * * continued eligibility@ means that prior to the end of the Medicaid recipient=s eligibility period as stated on the recipient=s recertification form, the recipient has been mailed a notice which states either (a) that the recertification has been processed and the recipient will have continued Medicaid eligibility until a date certain; or (b) that Defendants have received the recipient=s completed recertification form and that the recipient will have continuing Medicaid eligibility until further notice from Defendants.

22. If, after the conclusion of the work of Maximus Inc. required by paragraph 24 below and Defendants, having made all reasonable efforts for one year thereafter to comply with the standard set forth in paragraph 19 above, calculated by the method set forth in paragraph 21 above, have not achieved the standards set forth in those paragraphs, Defendants may move the Court to set an alternate standard to show compliance. Defendants shall have the burden to show that the standard set forth in paragraph 19, calculated by the method set forth in paragraph 21, cannot be achieved by all reasonable efforts.

23. No later than February 1, 1999, Maximus Inc. shall conduct quality control testing to ensure that the computer changes that Defendants have promised to make and that are required to implement this portion of the Order are fully operational and provide a report of their conclusions to Plaintiffs and the Monitor. The report of Maximus Inc. shall report in detail the type of quality control testing done and the results of the testing. In the event that Maximus Inc. does not complete the testing and provide a report to Plaintiffs and the Monitor by February 1, 1999, the Monitor shall no later than March 1, 1999, start conducting independent quality control testing to ensure that the computer changes that Defendants have promised to make and that are required to implement this portion of the Order are fully operational. The Monitor shall use his or her best efforts to engage a consultant who is familiar with ACEDS or a similar public benefits computer system. The Monitor shall report in detail the type of quality control testing done and the results to the Court and counsel for the parties. Provided however, that the parties intend to conduct a meeting in good faith after the execution of this Order for the purpose of eliminating the need for and cost of the study required in this paragraph. If the parties agree that the study required by this paragraph is not necessary in light of their meeting, they will execute a subsequent agreement to be approved by the Court eliminating this paragraph.

24. Defendants have entered a contract with Maximus Inc., pursuant to which Defendants have instructed Maximus Inc. that Maximus Inc. must study and prepare a report and recommendations concerning the actions Defendants will need to take in processing recertifications to comply with paragraph 19 above. Defendants shall ensure that the work of Maximus Inc. is completed on an expedited basis and a

report and recommendations submitted no later than February 1, 1999. Defendants shall provide Plaintiffs' counsel with a copy of the report and recommendations once completed within fifteen (15) days of receipt from Maximus Inc.

25. Defendants shall include in a written notice to all Medicaid applicants, and in a written notice to all Medicaid recipients at the time of recertification, a conspicuous statement that, if the recipient returns the recertification form and all required information and documentation prior to the end of the eligibility period, the recipient's eligibility must be continued uninterrupted until the recipient receives a notice of termination that states Defendants' determination that the recipient is no longer eligible for Medicaid. The notice shall also include information about other rights such as the right to a hearing, if there is an adverse determination on eligibility.

25A. ***Added by Order of August 8, 2000:*** Beginning no later than August 15, 2000, Defendants shall promptly register the receipt of completed recertification forms received from Medicaid recipients in the ACEDS computer system. No later than three business days after the registration in ACEDS of a completed recertification form, Defendants shall mail the recipient a notice, in the form set forth in Attachment A hereto, informing the recipient that Defendants have received a complete recertification form, that the recipient continues to be covered by Medicaid and will not be terminated from Medicaid until further notice from Defendants.

25B. ***Added by Order of August 8, 2000:*** Beginning no later than September 30, 2000, Defendants shall provide written notice to Medicaid recipients in the recertification form, in the form set forth in Attachment B

hereto, informing the recipient that once Defendants have received a complete recertification form, the recipient will receive a written notice from Defendants.

26. The notice required in paragraph 25 above shall include a conspicuous statement that if the recipient's Medicaid eligibility is terminated without advance notice or after notice that erroneously states that the recipient did not return the recertification form or all information and/or documentation requested, the applicant may obtain free legal assistance by contacting Plaintiffs' counsel. This statement shall give the name, address and telephone number of Plaintiffs' counsel. The reasonable time and expenses of Plaintiffs' counsel shall be deemed compensable monitoring of this Order under 42 U.S.C. ' 1988.

27. ***Revised by Order of August 8, 2000:*** Beginning no later than August 15, 2000, and on the 15th day of each month thereafter, Defendants shall submit to the Court, the Monitor, and Plaintiffs' counsel, a monthly report for each DHS service center handling recertifications (reporting the Multinational Unit separately as long as it exists). The monthly report shall include the following information for each recipient whose Medicaid eligibility was determined as a result of a recertification (i.e., approved or terminated) during the previous month: (a) in alphabetical order, the name, address, telephone number (if known), and Medicaid identification number for each such recipient; (b) the date any recertification form(s) was mailed to the recipient; (c) the date the recipient's then current eligibility period began; (d) the date the recipient's then current eligibility period expires; (e) the date that the completed recertification form is registered in the ACEDS computer system; (f) the date Defendants mailed any notice to the recipient that a complete recertification form had been received; (g) the date that Defendants determined (i.e., approved or

terminated) the recipient's eligibility; and (h) the date that any advance notice(s) of termination or continued eligibility was mailed to the recipient. In addition, the report shall set forth in composite form the total number of recertification forms received back from recipients in the month, the number approved in the month, and the number terminated in the month.

28. Defendants have contracted with Maximus Inc. to issue a report and recommendations concerning the production of the reports required by paragraph 27 above. Upon receipt and review of that report, Plaintiffs agree to engage in good-faith negotiations with Defendants concerning whether the reports required by paragraph 27 can be made less burdensome to Defendants while still meeting Plaintiffs' legitimate information needs. If Defendants propose a modification to the reports required by paragraph 27 and the parties cannot agree, Defendants may submit the matter to the Court for resolution. Defendants shall have the burden of proof to show that Plaintiffs' need for the particular information in order to enforce this Order is outweighed by the costs of providing such a report.

IV. Eligibility Verification System (EVS)

29. Defendants shall not operate the Eligibility Verification System (EVS) in a manner that causes eligible Medicaid recipients' benefits to be terminated, suspended, or interrupted without advance notice or an opportunity for a hearing. Defendants shall instruct its providers that they must call the EVS backup system if EVS reports ineligibility. Defendants shall state in the Rights and Responsibilities sheet that providers have been so instructed.

30. Defendants shall include in a document provided at the time the application is made to each applicant (including those who mail in applications or submit them at a location other than a Department of Human Services service center), in notices of eligibility, and in recertification forms or accompanying written materials, a conspicuous statement that, if, during a period when they are eligible for Medicaid, EVS informs the recipient or a provider is informed that the recipient is not eligible for Medicaid, the recipient may obtain free legal assistance by contacting Plaintiffs' counsel. This statement shall give the name, address and telephone number of Plaintiffs' counsel. Defendants shall provide this same information, at least annually, to all Medicaid providers and require the providers to provide Medicaid recipients with this same information if EVS reports them as ineligible for Medicaid during a period when they are eligible. The reasonable time and expenses of Plaintiffs' counsel shall be deemed compensable monitoring of this Order under 42 U.S.C. ' 1988.

31. On the 15th of each month, Defendants shall submit to the Monitor, and Plaintiffs' counsel, a monthly report of all systemic problems experienced by EVS, including but not limited to, breakdowns and failures of the system to provide needed information in a timely manner.

32. Defendants shall conduct quality control of the EVS system and make monthly reports to the Monitor and Plaintiffs' counsel regarding the results of the quality control. Defendants shall be deemed in compliance with this portion of this Order only if they can establish through a statistically valid sampling method that the verification system, including both EVS and the back-up system, accurately confirms the eligibility status of at least 98% of all requests for eligibility verification in any given month.

33. Defendants shall maintain a consistently accurate back-up system that can be used when EVS and/or its replacement states that a person is ineligible. The back-up system shall include a telephone information service that shall provide Medicaid recipients and providers with all eligibility information provided by EVS or its replacement, twenty-four (24) hours a day, three hundred and sixty-five (365) days a year. Defendants shall direct providers to use the back-up system whenever EVS reports ineligibility. Defendants shall notify recipients of the existence and purpose of the back-up system and its telephone number in the notices approving the recipient's eligibility and recertification. Defendants shall notify providers of the existence and purpose of the back-up system and its telephone number in a Transmittal at least annually.

34. If the reports submitted by Defendants under paragraph 32 above show that the verification system, including both EVS and the back-up system, accurately confirms the eligibility status of at least 98% of all requests for eligibility verification for twenty-two (22) of twenty-four (24) consecutive months, and accurately confirms the eligibility status of at least 95% of all requests for each of the other two (2) months, Defendants shall no longer be required to submit the reports required by paragraphs 31 and 32 above. These consecutive months shall begin with the first report showing at least 98% accuracy, including any such months before the effective date of this Order. However, after Defendants cease producing such reports on a monthly basis, Plaintiffs may choose one month per calendar year for Defendants to produce the reports required by paragraphs 31 and 32. If the single month's report shows compliance with the 98% standard, no further reports may be required until the subsequent calendar year. If the single report shows that the

98% standard is not being met, Defendants shall produce the monthly reports required by paragraphs 31 and 32 until Defendants have shown six (6) consecutive months of compliance with the 98% standard. Defendants shall not be in violation of this paragraph in any month in which an event beyond the reasonable control of Defendants causes Defendants to fail to comply with this paragraph, such as a central computer breakdown. In such an event, such a month shall not be considered in determining compliance with this paragraph or the termination of this paragraph under paragraph 76 below. No event shall satisfy the requirements of this paragraph unless Plaintiffs' counsel is notified in writing of the claim and the justification for the claim (a) within fourteen (14) days of Defendants having actual notice that the event will cause failure to comply with this paragraph, or (b) within twenty-two (22) days of the end of the reporting month affected by the event, whichever is sooner.

35. If Defendants fail to meet the deadlines or other requirements set forth in paragraphs 29, 30 and 32-34 above, Defendants shall submit to Plaintiffs, within fourteen (14) days, a report specifically describing the failure, the reasons for the failure, a schedule for correcting the failure, and the measures that will be taken to prevent the failure in the future. If Defendants fail to submit the report or Plaintiffs notify the Monitor that they are not satisfied with the report, the Monitor shall study the reasons for such failure and possible remedies and submit recommendations to the Court for implementation by Defendants. The parties shall have thirty (30) days thereafter within which to submit comments on the Monitor=s recommendations, and prior to the Court taking any action.

V. EPSDT Services (Claim 6)[1/]

36. Defendants shall provide or arrange for the provision of early and periodic, screening, diagnostic and treatment services (EPSDT) when they are requested by or on behalf of children.

37. Within thirty (30) days after the effective date of each contract, Defendants shall ensure that the Managed Care Organizations (MCO's) with which it contracts to provide EPSDT services to children maintain a tracking system for all children that shows:

(a) by name and Medicaid identification number, whether each child has obtained the screens, as defined in 42 U.S.C. 1396d(r)(1)(B), and laboratory tests set forth in the District of Columbia periodicity schedule issued in accordance with 42 U.S.C. 1396d(r)(1)(A)(i),1396d(r)(2)(A)(i),1396d(r)-(3)(A)(i), 1396d(r)(4)(A)(i), at the times set forth in that schedule, including lead blood screens, mental health screens, dental services, and vision and hearing tests (hereafter "screens and laboratory tests");

(b) by name and Medicaid identification number, whether each child has received age-appropriate immunizations in accordance with the immunization schedule of the Centers for Disease Control Advisory Committee on Immunization Practices (hereafter "immunization schedule");

1/The following provisions in this Section of the Order shall relate to all Medicaid recipients under the age of twenty-one (21) (hereafter Achild@ or Achildren@).

(c) by name and Medicaid identification number, whether and on what date(s) each child has been referred for corrective treatment determined to be necessary as a result of an EPSDT screen or laboratory test;

(d) by name and Medicaid identification number, whether and on what date each child referred for corrective treatment as a result of an EPSDT screen or laboratory test has obtained the corrective treatment for which the child was referred;

(e) by name and Medicaid identification number, the date on which each of the outreach activities set forth in paragraphs 38 and 39 below were undertaken with respect to the child.

38. The contracts that Defendants are entering into with MCO's in 1998 require that the MCO's:

> shall conduct outreach activities to assist enrollees make and keep EPSDT appointments for eligible children. The outreach activities shall include every reasonable effort, including telephone calls, scheduling of appointments for recipients, mailed reminders and personal visits, to contact parents, guardians of children, or the children themselves, if appropriate, based on the child's age, who are due for, or who have failed to keep appointments for, EPSDT screens and laboratory tests set forth in the District's periodicity schedule, immunizations, or follow-up treatment to correct or ameliorate a defect identified during an EPSDT screen or laboratory test, or have otherwise not obtained EPSDT screens[,] laboratory tests, immunizations, follow-up treatment or other services, in order to assist them to obtain such services.

Defendants shall monitor these activities and enforce these contractual provisions in order to assure that they are fully carried out.

39. Defendants shall require all MCO's in all contracts entered, renewed, extended and/or modified after January 1, 1999, to make every reasonable effort to contact parents, guardians of children, or the children themselves, if appropriate, based on the child's age, who are due for, or who have failed to keep appointments for, EPSDT screens and laboratory tests set forth in the District of Columbia periodicity schedule issued in accordance with 42 U.S.C. 1396d(r)(1)(A)(i), 1396d(r)(2)(A)(i), 1396d(r)(3)(A)(i), 1396d(r)(4)(A)(i), immunizations, or follow-up treatment to correct or ameliorate a defect identified during an EPSDT screen or laboratory test, or have otherwise not obtained EPSDT screens, laboratory tests, immunizations, follow-up treatment or other services, in order to assist them to obtain such services. Such contracts shall provide that "every reasonable effort" shall include, at a minimum, a telephone call or mailed reminder prior to the due date of each visit, scheduling of appointments for recipients, and, in the case of a missed appointment, a telephone call or mailed reminder for the first missed appointment and, if there is no response, a personal visit to urge the parent or guardian to bring the child for his or her EPSDT appointment. The contracts may provide that a personal visit need not be made if the MCO determines that the specific neighborhood or apartment building is dangerous for such a visit during the particular time of day involved and the MCO retains documents that state the specific reasons why no personal visit was made. The contracts need not (a) require the MCO's to make useless efforts to contact Medicaid recipients using these methods, such as telephone calls need not be made if it is known that the recipients have no telephone or mailings need not mailed or personal visits attempted if an address for the recipient cannot be ascertained after reasonable efforts to obtain it, or (b) preclude the MCO's from taking other actions to contact

Medicaid recipients. The contracts shall also require MCO's to maintain records showing the information set forth in paragraph 37 above and the efforts made to assist recipients to obtain EPSDT services that are set forth in this paragraph. Plaintiffs' counsel shall have access to these records through Defendants' counsel to ensure that MCO's are complying with this paragraph. While these requirements shall be explicitly set forth in the contract, the contract need not include the exact language of this paragraph. Defendants shall monitor these activities and enforce these contractual provisions in order to ensure that they are fully carried out.

40. If the definition of "every reasonable effort" set forth in paragraph 39 above proves infeasible or ineffective after two years under contracts including that definition, either party may inform the other party and the parties shall attempt in good faith to agree on an alternate definition. If the parties' efforts are not successful after thirty (30) days, either party may bring the issue to the Monitor. The Monitor shall report to the Court on the issue. Each party shall have thirty (30) days from the date of the Monitor's report to comment before the Court takes any action.

41. Defendants shall ensure that the MCO's train all EPSDT providers, during the first year of the contract and at least biannually thereafter, about the current requirements for EPSDT and shall develop a monitoring program for the purpose of ensuring, on at least a biannual basis, that each physician providing EPSDT services has the necessary equipment and knowledge to perform such services in accordance with standard medical practice. Defendants shall send any HCFA directions or guidance relevant to an MCO's obligation to implement the EPSDT program to each MCO within a reasonable time after receipt, not to

exceed thirty (30) days unless unusual circumstances (such as the need to seek clarification from HCFA) make such transmittal in thirty (30) days unreasonable. Defendants shall direct each MCO to provide such information, when relevant, to each EPSDT provider within the MCO's network within ten (10) days of receipt by the MCO. Defendants shall report the activities of the monitoring program to the Court, the Monitor and Plaintiffs' counsel, annually, with the first report due no later than June 1, 1999.

42. Defendants shall provide each physician participating in the EPSDT program with a list of specialists to whom referrals may be made for screens, laboratory tests and corrective treatment. Defendants shall operate a telephone information service that functions during normal business hours to respond to inquiries from providers and EPSDT recipients or their parents or guardians concerning EPSDT referrals.

43. The contracts that Defendants are entering into with MCO's in 1998 provide that:

(a) the MCO shall meet a 75% participant ratio, as defined by the HCFA State Medicaid Manual, Section 5360.B and computed in accordance with the HCFA State Medicaid Manual, Section 2700.4 (hereafter "participant ratio") for 1998 for all children enrolled with the MCO.

(b) the MCO shall meet an 80% participant ratio for 1999 for all children enrolled with the MCO.

(c) Each screen, laboratory test and immunization must be conducted within sixty (60) days of its due date, based on the child's age, under the periodicity schedule or immunization schedule for all

children over the age of two (2) years and within thirty (30) days of its due date for all children under the age of (2) two years.

44. The contracts that Defendants are entering into with MCO's in 1998 further provide that:

b. If Provider fails to meet or show progress toward meeting the EPSDT performance standards in paragraph "a" of this section or ensure that children have their age-appropriate screens updated for missed opportunities, the District shall take any or all of the following actions (depending on the extent of the failure to comply or to demonstrate progress with the standards):

(1) require the Provider to develop and implement a corrective action plan, that is approved by the District and is designed to increase Provider's EPSDT participation ratio;

(2) require the Provider to utilize the Department's EPSDT case management program; or

(3) withhold an amount from the Provider's payment, pursuant to Article 11, section A.3 at a rate of $45 for each enrollee that is required to be added to the numerator in Provider's EPSDT participation ratio to comply with the performance standards in paragraph "a" of this section.

If any MCO fails to comply with the participant ratio percentage set forth in paragraph 43 above, Defendants shall take the following actions:

(a) In fiscal year 1998, if the MCO has a participant ratio of less than 65%, it shall be required to develop and implement an effective corrective action plan;

(b) In fiscal year 1999, if the MCO has a participant ratio of less than 70%, it shall be required to develop and implement an effective corrective action plan and, if the MCO has a participant ratio of less than 60%, it shall also be required to pay Defendant at a rate of $45 for each enrollee that is required to be added to the numerator in the MCO's EPSDT participant ratio to meet the 70% requirement in the contract.

Plaintiffs' counsel shall have the opportunity to comment within 15 days of their receipt of any corrective action plan before approval by Defendants. Defendants shall enforce these contractual requirements and the corrective action plans.

Defendants shall inform the MCO of the date that they have provided the corrective action plan to plaintiffs. Plaintiffs shall keep any such corrective action plans confidential for a period of 15 days after receipt. During those 15 days, if the MCO believes that the corrective action plan contains confidential information, it may move this Court for an Order that the confidential portions of the corrective action plan be subject to a protective order. If such a motion is made by the MCO, plaintiffs shall keep the corrective action plan confidential until the resolution of the motion. The foregoing procedures concerning claims to confidentiality by MCO's do not affect defendants' obligations under the District of Columbia Freedom of Information law, D.C. Code ' 1-1521, et seq.

45. In all contracts entered, renewed, extended and/or modified with MCO's on or after January 1, 1999, Defendants shall, at a minimum, require the MCO's:

(a) to provide each EPSDT screen, laboratory test and immunization within sixty (60) days of its due date, based on the child's age, under the periodicity schedule or immunization schedule for all children over the age of two (2) years and within thirty (30) days of its due date for all children under the age of two (2) years.

(b) to meet an 80% participant ratio for fiscal year 1999 and thereafter for all children enrolled with the MCO.

(c) In fiscal year 2000, to develop and implement an effective corrective action plan if the MCO has a participant ratio of less than 75% and, if the MCO has a participant ratio of less than 65%, it shall also be required to pay Defendants at least at a rate of $45 for each enrollee that is required to be added to the numerator in the MCO's EPSDT participant ratio to meet the 80% requirement.

(d) In fiscal year 2001, to develop and implement an effective corrective action plan if the MCO has a participant ratio of less than 80% and, if the MCO has a participant ratio of less than 70%, it shall also be required to pay Defendants at least at a rate of $45 for each enrollee that is required to be added to the numerator in the MCO's EPSDT participant ratio to meet the 80% requirement.

(e) In fiscal year 2002 and any year thereafter, to develop and implement an effective corrective action plan if the MCO has a participant ratio of less than 80% and, if the MCO has a participant rate of less than 75%, it shall also be required to pay Defendants at least at a rate of $45 for each enrollee that is required to be added to the numerator in the MCO's EPSDT participant ratio to meet the 80% requirement.

Plaintiffs' counsel shall have the opportunity to comment on any corrective action plan before approval by Defendants. Defendants shall enforce these contractual requirements and the corrective action plans.

(f) If in soliciting bids or negotiating modifications to the contracts described in this paragraph, Defendants cannot secure such contracts or such modifications without an increase in cost above the federal upper payment limit for capitation rates as a result of the requirements set forth in this paragraph and paragraph 39, Defendants may move the Court to modify the requirements set forth in this paragraph and in paragraph 39. In making any such motion, Defendants shall bear the burden to show that the requirements of this paragraph and paragraph 39 are the provisions which caused the upper payment limit to be exceeded.

46. Defendants shall comply with the HCFA State Medicaid Manual, Section 2700.4, in completing the HCFA Form 416. Defendants shall ensure that MCO's comply with the HCFA State Medicaid Manual, Section 2700.4, in providing information to be used in the HCFA Form 416 relating to whether the participant ratios in paragraphs 43, 44, and 45 above have been complied with. Defendants shall include a provision in the contracts with MCO's that requires the MCO's to submit to Defendants adequate information for Defendants to produce the reports required by paragraph 47 below. Defendants shall use an independent party to verify annually the data from each MCO used to compile the HCFA Form 416 used by Defendants to determine the participant ratios in paragraphs 43, 44, and 45. Defendants shall provide the results of the verification and the data for each MCO to Plaintiffs' counsel.

46A. Defendants shall direct the MCO=s to prepare any corrective action plan required pursuant to terms of this Order no later than April 1 of the year following the fiscal year completed on September 30 in which the MCO=s performance gives rise to the requirement to prepare a corrective action plan. Defendants shall direct the MCO=s to submit a corrective action plan required pursuant to terms of this Order no later than 30 days following the date that Defendants inform the MCO that a corrective action plan is required, *i.e.*, by May 1. *[46a Added by Order of October 18, 2000]*

47. Defendants shall provide quarterly reports to the Court, the Monitor, and Plaintiffs on the provision of EPSDT services. The reports shall contain the following information for each MCO:

(a) Number of individuals eligible for EPSDT enrolled with the managed care organization (MCO). The total unduplicated number of individuals under age 21 determined to be eligible for Medicaid, distributed by age (as defined in the line 1 instructions for the HCFA Form 416 set forth in the HCFA State Medicaid Manual, Section 2700.4). Unduplicated means that an eligible individual is reported only once, although he or she may have had more than one period of eligibility during the reporting period.

(b) Number of individuals receiving at least one initial or periodic screening service from the MCO. The unduplicated count of individuals, distributed by age, who received one or more documented initial or periodic screenings (as defined in the line 7 instructions for the HCFA Form 416 set forth in the HCFA State Medicaid Manual, Section 2700.4) during the quarter.

(c) Actual Number of Initial and Periodic Screening Services. The number of initial and periodic EPSDT child health screening examinations during the quarter (as defined in the line 10 instructions for the HCFA Form 416 set forth in the HCFA State Medicaid Manual, Section 2700.4).

(d) Number of individuals referred for corrective treatment. The unduplicated count, distributed by age, of individuals who, as the result of at least one health problem identified during an EPSDT child health screening, excluding vision, dental, and hearing services, were

scheduled for another appointment with the screening provider or referred to another provider for further needed diagnostic or treatment service (as defined in the line 12 instructions for the HCFA Form 416 set forth in the HCFA State Medicaid Manual, Section 2700.4). This does not include correction of health problems during the screening examination or referrals for vision, dental, and hearing services.

(e) Number of individuals receiving corrective treatment. The unduplicated count, distributed by age, of EPSDT-eligible individuals who received corrective treatment from a specialist.

(f) Number of individuals receiving vision assessments. The unduplicated count, distributed by age, of individuals who received an assessment to determine the need for diagnosis and treatment for defects in vision (as defined in the line 13 instructions for the HCFA Form 416 set forth in the HCFA State Medicaid Manual, Section 2700.4).

(g) Number of individuals receiving dental assessments. The unduplicated count, distributed by age, of individuals who received preventive dental services (as defined in the line 14 instructions for the HCFA Form 416 set forth at HCFA State Medicaid Manual, Section 2700.4).

(h) Number of individuals receiving hearing assessments. The unduplicated count, distributed by age, of individuals who received an assessment to determine the need for diagnosis and treatment for defects in hearing (as defined in the line 15 instructions for the HCFA Form 416 set forth in the HCFA State Medicaid Manual, Section 2700.4).

The first report shall be due on October 1, 1998, and shall cover April 1, 1998, through June 30, 1998. Thereafter, reports shall be due one hundred and twenty (120) days after the conclusion of each quarter. In addition, Defendants shall produce to Plaintiffs the HCFA Form 416 for each year within fourteen (14) days of its submission to the federal government.

48. (a) The covenants, corrective action plans, and penalties set forth in paragraphs 44 and 45 above are intended as the actions reasonably required of Defendants for assuring that the MCO's, as far as possible, will attain a participant ratio of 75% for 1998 and 80% for 1999 and thereafter. However, the parties and the Court recognize that they do not have sufficient information and experience to be certain that these ratios can be attained, even if the MCO's and Defendants take such actions. It may be that the participant ratios required in paragraphs 43(a) and (b) and 45(b) are attainable through the enforcement mechanisms prescribed in paragraphs 44 and 45, but they may be unattainable despite such enforcement mechanisms. This paragraph is therefore intended to provide a mechanism to determine whether the actions of Defendants and the MCO's under this Order constitute a reasonable effort, consistent with this Order, to achieve the participant ratios required under the MCO contracts and this Order. When such participation deficits occur, the Court will scrutinize Defendants' performance in achieving the specified participant ratios if, but only if, the participant ratios achieved are under 60% in 1999, 65% in 2000, 70% in 2001, 75% in 2002 and 80% in 2003 and each year thereafter.

(b) Defendants shall calculate the participant ratio for fiscal year 1998, which shall become the base year. If, in any subsequent year, the percentage ratio for that year set forth in subparagraph (a) above is not met and the ratio is also less than the 1998 base year ratio plus 5% for each subsequent year (but not more than 80%) (e.g., for 2000, the figure is the 1998 participant ratio, plus 10%), Defendants shall by June 15 of the following year, provide a detailed explanation to Plaintiffs of (i) the actions taken by the MCO's in 1998 and subsequent years through the year in issue to meet the relevant participant ratio in paragraphs

43(a) and (b) and 45(b), and (ii) whether it would be reasonable and effective to direct Defendants to require the MCO's to take further actions that are consistent with the MCO contracts. *[48(b) Revised by Order of October 18, 2000]*

(c) If Plaintiffs are satisfied with Defendants' explanation, Defendants shall be deemed in compliance with the participant ratio for that year. If Plaintiffs are not satisfied with Defendants' explanation, they may prepare a written response and present it, along with Defendants' explanation, to the Monitor. The Monitor will then consult with the parties and prepare a report to the Court addressing whether it would be reasonable and effective to direct Defendants to require the MCO's to take further actions consistent with the MCO contracts. The Monitor's report shall be due within 30 days of the issue being presented to the Monitor.

(d) The parties shall have thirty (30) days after submission of the Monitor's report to the Court within which to submit comments on such report. If the Court determines that it would be reasonable and effective, in order to achieve a participant ratio meaningfully higher than in the previous year, to direct Defendants to require the MCO's to take further actions consistent with the MCO contracts, the Court shall determine what relief, if any (other than contempt sanctions), shall be afforded to Plaintiffs. If, on the other hand, the Court determines that directing further actions consistent with the MCO contracts would be either unreasonable or ineffective in achieving a participant ratio meaningfully higher than in the previous year, Defendant shall be deemed in compliance with the participant ratio for that year. However, in this latter event, if the Court concludes that there are further actions that would be reasonable and effective in

achieving such a meaningfully higher participant ratio, but that such actions are unavailable under the terms of the MCO contracts, Plaintiffs may, upon motion, seek further relief from the Court that Defendants, under the circumstances, could reasonably be expected to provide.

49. Defendants' periodicity schedule shall require dental services at least annually for children age six (6) through twenty (20).

50. Defendants shall follow the federal requirements set forth in the HCFA State Medicaid Manual, Section 2700.4, in reporting line 12 on the HCFA Form 416 concerning referrals or comparable provisions in future forms for treatment of conditions discovered in the course of EPSDT screens and laboratory tests.

51. ***Revised by Order of July 25, 2000:*** Beginning no later than the date of entry of this Order, Defendants shall offer scheduling and transportation assistance prior to the due date of each eligible child's periodic screening, laboratory tests and immunizations as required by the HCFA State Medicaid Manual, Section 5150. The offer of scheduling and transportation assistance may be made in conjunction with another communication prior to the due date of each eligible child's periodic screening, laboratory tests and immunizations.

52. Beginning no later than the date of entry of this Order, Defendants shall assure that children and their parents or guardians shall be provided assistance, when requested and necessary, with transportation to EPSDT appointments.

53. Beginning no later than the effective date of each of the MCO contracts Defendants shall ensure that the MCO's provide case management services, as described in the HCFA State Medicaid Manual ' 4302 and as defined by 42 U.S.C. 1396n(g)(2), to children with a need for such services under the EPSDT program. No later than January 15, 1999, and no later than July 15, 1999, Defendants shall report to the Monitor and Plaintiffs' counsel concerning the implementation of case management services to children with a need for such services under the EPSDT program. Defendants shall consider in good faith any comments by Plaintiffs' counsel concerning its provision of case management services under the EPSDT program.

VI. EPSDT Notice (Claim 7)[1/]

54. Defendants shall effectively inform all pregnant women, parents, child custodians, and teenagers who are sui juris and who have been determined to be eligible for Medicaid benefits, including individuals who are blind or deaf, or who are illiterate, of the availability of early and periodic, screening, diagnostic, and treatment services (hereafter AEPSDT@) and the need for age-appropriate immunizations against vaccine-preventable diseases. Notice shall be provided to all such individuals, to all applicants for Medicaid, and to all Medicaid recipients, at least annually, in writing. In addition, oral notice must be given at least annually if such individual meets with a social service representative. The oral and written notice shall use clear and non-technical language, and shall be designed to effectively inform EPSDT-eligible individuals about the benefits of preventive care, the services available under the EPSDT program, where and how to obtain those services, the cost-free nature of the services, and the availability of necessary scheduling and transportation assistance.

2/The following provisions in this Section of the Order shall relate to all Medicaid recipients under the age of twenty-one (21) (hereafter Achild@ or Achildren@).

55. Defendants shall establish and maintain a helpline that explains EPSDT services in Spanish which is available whenever no Spanish-speaking DHS employee is available to give an oral explanation and the person to whom notice is to be given understands only Spanish.

56. Defendants shall develop a program, to be implemented by February 1, 1999, to provide adequate notice about the EPSDT program to eligible persons who are blind or deaf, and who cannot read or cannot understand English. Defendants submitted the plan to the Court, the Monitor and Plaintiffs' counsel on March 16, 1998, and Plaintiffs have provided Defendants and the Monitor with their response to the Plan. If the parties are unable to agree on the terms of the Plan and its implementation, the Monitor shall evaluate the Plan and submit a report on the Plan and its implementation to the Court and counsel. The parties shall have fifteen (15) days thereafter within which to submit comments on the report, and prior to the Court taking any action.

57. Defendants shall require all providers of Medicaid services to give all pregnant women, parents, child custodians, and teenagers who are sui juris, and who have been determined to be eligible for Medicaid benefits, including individuals who are blind or deaf, or who are illiterate, written material describing EPSDT services in simple terms when they first visit the provider and on subsequent visits, unless the provider has given the recipient such material within the preceding year. Defendants shall also require all providers of Medicaid services to explain the EPSDT program orally to such recipients at least annually to all recipients who use Medicaid services during the year, except that so long as the Defendants' periodicity schedule requires only biannual EPSDT screening for children over the age of six (6), such children, and/or

their parents or guardians, need only be orally informed about EPSDT biannually. Defendants shall require providers to call the Spanish helpline described above whenever the person to whom notice is to be given understands only Spanish.

58. The written and oral notices set forth in paragraphs 54, 55 and 57 above shall include:

(a) An explanation of all EPSDT medical services, including screens, laboratory tests, immunizations and corrective treatment;

(b) An explanation of the importance of these services, and a strong recommendation that the services be utilized;

(c) An explanation of the right of the child to follow-up treatment to correct or ameliorate any medical need identified during a screen or laboratory test;

(d) An explanation of the right to scheduling assistance in order to make EPSDT appointments and the procedures for obtaining such assistance; and

(e) An explanation of the right to transportation assistance and the procedures for obtaining such assistance for EPSDT appointments.

In addition, Defendants shall provide EPSDT eligible applicants at the time of application and at least annually thereafter, a pocket-sized schedule of EPSDT screens, laboratory tests and immunizations.

59. Beginning no later than November 15, 1998, Defendants shall develop and implement effective coordination of EPSDT notice and outreach with the Department of Health, the District of Columbia public school system, Headstart programs, the Women, Infants and Children nutrition program,

public housing programs, Title XX programs, and the District's Part H early intervention program. The plan for coordination shall be provided to the Court, the Monitor and Plaintiffs' counsel within ten (10) days of its completion. The Monitor shall submit, within fifteen (15) days thereafter, an evaluation of the coordination plan, and shall monitor its implementation.

60. Plaintiffs may submit to the Court at any time after October 15, 1998, information concerning the effectiveness of EPSDT notice in the District of Columbia. If the Court determines that Plaintiffs have raised a substantial issue as to such effectiveness, the Court shall request the Monitor to submit a report on appropriate measures to improve such effectiveness, including the need for, the feasibility and mechanics of, and the cost of a statistically valid study of the effectiveness of EPSDT notice in the District of Columbia. The parties shall have thirty (30) days after the submission of the Monitor's report within which to submit comments on such report, and prior to the Court taking any action. "Effectiveness of EPSDT notice" as used in this paragraph shall have the same meaning as the phrase "to inform effectively all EPSDT eligible individuals (or their families) about the EPSDT program" as set forth in 42 C.F.R. 441.56(a).

VII. Reimbursement Procedure for Class Members= Expenses

61. Defendants' Medicaid State Plan shall allow for corrective payments to Medicaid recipients who have incurred out-of-pocket medical expenses that, but for Defendants' error, should have been paid by Medicaid.

62. Defendants shall provide corrective payments to Medicaid recipients who have incurred out-of-pocket medical expenses that should have been paid by Medicaid to all current and future Medicaid recipients and all those who were Medicaid recipients or were eligible for Medicaid at any time since March 2, 1990. Reimbursement of class members shall be made when the class member presents reasonable and reliable documentation or other evidence of their out-of-pocket expenses.

63. In an Order dated September 15, 1997, after considering the Monitor's report and the positions of the parties, the Court issued a Reimbursement Procedures Order setting forth the procedures for reimbursing Medicaid recipients for out-of-pocket expenses incurred since March 2, 1990. In an Order Partially Modifying the Reimbursement Procedures of the Amended Remedial Order of May 6, 1997, and the Reimbursement Procedures Order of September 15, 1997, entered on July 30, 1998, the Court set forth further procedures concerning reimbursement.

VIII. Monitoring Fees to Plaintiffs' Counsel

64. Plaintiffs' counsel may respond to all calls which come to their office and make reasonable inquiry to determine whether the caller is a member of the plaintiff class. If the caller is a member of the plaintiff class, Plaintiffs' counsel may provide the caller with legal assistance. The reasonable time and expenses of Plaintiffs' counsel in making such inquiry and providing such legal assistance shall be deemed compensable monitoring of this Order under 42 U.S.C. ' 1988 and applicable law interpreting that statutory provision. The hourly rate for handling the claims of individual class members shall be $75/hour, regardless of the experience level of the lawyer who performs the work. This hourly rate shall be adjusted annually, beginning on January 1, 1999, based on the U.S. Department of Commerce Consumer Price Index for Legal Services.

65. Other reasonable attorney time by Plaintiffs' counsel in monitoring Defendants' compliance with this Order shall be compensated at the rate of $315/hour for the time of Bruce J. Terris and Lynn Cunningham, and $265/hour for the time of Kathleen L. Millian and Jane Perkins. Reasonable paralegal time shall be compensated at the rate of $75/hour. If attorneys other than those mentioned specifically in this paragraph perform monitoring work, the parties shall use their best efforts to agree to an hourly rate for the attorney, which shall not exceed $200/hour. These hourly rates shall be adjusted annually, beginning on January 1, 1999, based on the U.S. Department of Commerce Consumer Price Index for Legal Services.

66. The rates set forth in paragraphs 64 and 65 above for Plaintiffs' monitoring of Defendants' compliance with this Order were based on compromise and the parties do not intend these rates to apply

for any purpose other than those set forth in paragraphs 64 and 65. Defendants take the position that the reasonable rates for Plaintiffs' counsel are lower than those set forth in paragraphs 64 and 65 and Plaintiffs take the position that the reasonable rates are higher.

67. Plaintiffs may make an application for monitoring fees and expenses no more frequently than every six (6) months. If the parties cannot agree on the amount of fees and expenses, Plaintiffs may make a motion to the Court thirty (30) days after submission of the fees application to Defendants. The first such application may be submitted at any time after July 1, 1998. In addition to the costs of monitoring Defendants= compliance with this Order, the first application shall include all other fees incurred in this action since January 1, 1998, excluding those specified in paragraph 69(b) below.

68. *Deleted by Order of July 30, 2001:* ~~Beginning on May 15, 1997, and continuing thereafter, Plaintiffs' counsel shall provide Defendants' counsel with a monthly statement of their fees and expenses associated with monitoring Defendants' compliance with the Remedial Order.~~

IX. Attorneys' Fees and Expenses through December 31, 1997

69. In full settlement of all claims by Plaintiffs for attorneys' fees and expenses through December 31, 1997, except as specifically stated below, Defendants agree to pay Plaintiffs a total of $1,600,000. The Court vacates the Judgment for $1,028,059.70 entered on March 12, 1998. Of the sum of $1,600,000, $611,940.30 was paid pursuant to the Consent Judgments of September 3, 1996, and January 14, 1997, and the Judgment of March 12, 1998. Defendants agree to pay Plaintiffs the remaining $988,059.70 within forty-five (45) days of the date of entry of the Consent Judgment submitted with this Order. This sum of $988,059.70 shall bear interest, as provided in 28 U.S.C. 1961, from March 12, 1998, until paid. The sum of $1,600,000 does not include the following:

(a) Payments made to Plaintiffs under the Consent Judgment Orders entered on June 2, 1997 ($18,968.75, plus interest), and September 15, 1997 ($15,100, plus interest);

(b) Plaintiffs' claim for reimbursement of their fees and expenses for monitoring the Partial Settlement Agreement of July 12, 1996, and the Agreement Pursuant to Paragraph 49 of the July 10, 1996, Partial Settlement Agreement, dated May 22, 1997, which have been incurred since May 8, 1997.

X. Future Change in Applicable Law and Motions for Modification

70. If Defendants believe that a change of law resulting in the elimination or reduction in federal funding or in the amendment or elimination of legal requirements affects any provision of this Order, and Defendants desire a modification of this Order, Defendants shall notify Plaintiffs' counsel. The notice shall specify the modification desired and the reasons therefor. If the parties cannot come to an agreement regarding the modification to this Order, the parties shall jointly move the Court, within ten (10) days of the District's notice to Plaintiffs, to determine the extent to which modification shall be made. The joint motion shall request that the Court establish an expedited briefing schedule and determination of this motion.

71. Except as provided in paragraph 70 above, either party shall have the right to move the Court for a modification of this Order at any time for any reason.

72. In determining motions for a modification of this Order under paragraphs 70 and 71 above, the general body of federal law governing motions to modify orders in contested matters pursuant to Rule 60(b) of the Federal Rules of Civil Procedure shall apply.

73. Defendants shall take no action contrary to this Order based on a proposed modification to this Order under paragraphs 70 and 71 above until this Court has determined the joint motion filed under paragraphs 70 and 71. If Defendants take or threaten to take such an action, Plaintiffs may seek injunctive relief from the Court. The only exception shall be if the federal government has eliminated or reduced funding to the District for a program subject to this Order and, as a result, the District has legally eliminated

or reduced such program. In that event, Defendants shall notify Plaintiffs that they propose to take such action at least five (5) days prior to the effective date of Defendant's proposed action.

XI. Termination of this Order

74. ***Revised by Order of August 8, 2000:*** As to Section II of this Order (Processing of Medicaid Applications (Claim 4)), this Order shall terminate when Defendants have satisfied the compliance standards set forth in paragraphs 8 and 12 above for three (3) consecutive years. The parties do not agree as to whether Defendants should receive credit against the three (3) consecutive years of compliance for the time period prior to July 1, 2000, the date that the revised format reports are to be prepared pursuant to paragraph 16 above. At a time when Defendants believe that their compliance has satisfied this paragraph=s requirements for termination of the Order, they shall inform plaintiffs in writing. The parties agree to negotiate in good faith concerning whether Defendants= record demonstrates compliance with this paragraph. If the parties cannot agree, Defendants may move the Court for a determination as to whether they have complied with this paragraph.

75. As to Section III of this Order (Processing of Medicaid Recertifications (Claim 5)), this Order shall terminate when Defendants have satisfied the compliance standard set forth in paragraph 19 above for three (3) consecutive years.

76. As to Section IV of this Order (Eligibility Verification System (EVS)(Claim 5)), this Order shall terminate when Defendants have shown that the verification system, including both EVS and the back-up system, have accurately confirmed the eligibility status of 98% of all requests for eligibility verification for

twenty-two (22) of twenty-four (24) consecutive months and accurately confirmed the eligibility status of at least 95% of all requests for each of the other two (2) months as provided in paragraph 34 above and have accurately confirmed the eligibility status of at least 98% of all requests for the one (1) month in the following calendar year chosen by Plaintiffs. If Defendants do not achieve at least 98% compliance in the month chosen by Plaintiffs, Section IV shall not terminate until Defendants have shown at least six (6) consecutive months of compliance with the 98% standard.

77. As to Sections V and VI of this Order (EPSDT Services (Claim 6) and EPSDT Notice (Claim 7)), this Order shall terminate when Defendants have complied for three (3) consecutive years beginning no earlier than fiscal year 1999 with the provisions of Sections V and VI and the participant ratio of the District of Columbia has been no less than 75% for the last year. Defendants may move to terminate Sections V and VI of this Order at any time after fiscal year 2001 if Defendants have complied for three (3) consecutive years with all the provisions of Sections V and VI, except those setting forth a particular participant ratio, even though they have not achieved a participant ratio of 75% for the last year, if they can show, based on persuasive evidence as to the actions taken by MCO's and Defendants, that a higher participant ratio cannot be achieved by further reasonable efforts. Defendants shall have the burden of proof.

78. All other provisions of this Order shall conclude at the same time as the last of the Sections identified in paragraphs 74-77 above.

XII. Continuing Jurisdiction

79. The Court shall retain jurisdiction of this matter to make any necessary orders enforcing or construing this Order.

80. Before any party moves the Court to enforce or construe this Order, or pursuant to any provision in this Order, except for paragraph 73 above, it shall give the other party 10 days' notice of its intention. During that 10-day period, the parties shall negotiate in good faith in an effort to resolve the dispute without seeking a decision from the Court.

XIII. Construction of This Order

81. This Order shall be construed by its own terms. The presence or absence of a provision in the Court's previous orders or in any draft of this Order shall not be relevant to the meaning of the provisions of this Order.

XIV. Other Matters

82. All references to the HCFA State Medicaid Manual shall be to the current manual at the time of the event involved.

83. The Court recognizes that computer software programs which are date dependent may experience failures in operations as the year 2000 commences, the so-called Y2K disruption, despite the Defendants taking reasonable efforts to identify and correct such problems in advance. Should such disruptions prevent the Defendants from complying with any requirement of this Order, despite Defendants taking reasonable efforts to identify and correct such problems in advance, upon notice to the Court, the Monitor, and Plaintiffs, Defendants shall have the right to suspend the provisions of the Order affected

during the first six (6) months of 2000. No month during which such provisions are suspended may be used to justify termination under Section XI of this Order as to the provisions suspended. If Defendants invoke this suspension, they must, within 30 days of giving the required notice, report to the Court, the Monitor and Plaintiffs of the efforts they have taken to date and any planned in the future to identify and correct the Y2K disruption.

AGREED:

Date: _1/8/99_____

___/s/_____
BRUCE J. TERRIS, Bar #47126
KATHLEEN L. MILLIAN, Bar #412350
LYNN E. CUNNINGHAM, Bar #221598
Terris, Pravlik & Millian, LLP
1121 12th Street, N.W.
Washington, D.C. 20005
(202) 682-2100

JANE PERKINS
NATIONAL HEALTH LAW PROGRAM
211 N. Columbia St., 2nd Floor
Chapel Hill, NC 27514
(919) 968-6308

ROBERT BERLOW, Bar #928069
805 Fairfield Estates Court
Crownsville, MD 21032

Date: __1/8/99_____

____/s/_____
JOHN M. FERREN
Corporation Counsel, D.C.

CHARLES L. REISCHEL
Deputy Corporation Counsel, D.C.
Appellate Division

WILLIAM J. EARL [CD-MC]
Assistant Deputy Corporation Counsel, D.C.
Special Litigation Division

ROBERT C. UTIGER
Assistant Corporation Counsel
441 4th Street, N.W., Rm. 6SO96
Washington, D.C. 20001

(301) 912-2281 (202) 727-6295 ext. 3457

Counsel for Plaintiffs Counsel for Defendants

APPROVED AND ENTERED AS AN ORDER OF THIS COURT THIS 22nd DAY OF

January, 1998~~9~~9.

/s/
GLADYS KESSLER
United States District Judge

Copies to:

Bruce J. Terris
Kathleen L. Millian
Lynn E. Cunningham
Terris, Pravlik & Millian, LLP
1121 12th Street, N.W.
Washington, D.C. 20005

Robert Berlow
805 Fairfield Estates Court
Crownsville, MD 21032

Jane Perkins
National Health Law Program
211 N. Columbia St., 2nd Floor
Chapel Hill, NC 27514

Robert C. Utiger
Assistant Corporation Counsel, D.C.
One Judiciary Square - Room 6S096

441 - 4th Street, N.W.
Washington, D.C. 20001

Jesse Goode
General Counsel
Department of Human Services
801 East Building
Suite 2000
2700 Martin Luther King Ave., S.E.
Washington, D.C. 20032

ATTACHMENT A

Your completed recertification for Medicaid/DC Healthy Families/Medical Charities/QMB was received on _____. Medical Assistance for your household will continue without change until further notice from this agency. When a decision is made concerning your household=s continued eligibility, you will receive a notice informing you of the results.

ATTACHMENT B

You will receive a notice from us when we receive your completed recertification form, letting you know that we have received it.

GOVERNMENT OF THE DISTRICT OF COLUMBIA

STANDARD CONTRACT PROVISIONS

FOR USE WITH

DISTRICT OF COLUMBIA GOVERNMENT
SUPPLIES AND SERVICES CONTRACTS

March 2007

OFFICE OF CONTRACTING AND PROCUREMENT
SUITE 700 SOUTH
441 4th STREET, NW
WASHINGTON, DC 20001

STANDARD CONTRACT PROVISIONS

TABLE OF CONTENTS

1. Covenant Against Contingent Fees: *1*
2. Shipping Instructions – Consignment: *1*
3. Patents: *1*
4. Quality: *1*
5. Inspection Of Supplies: *1*
6. Inspection Of Services: *3*
7. Waiver: *4*
8. Default: *4*
9. Indemnification: *6*
10. Transfer: *6*
11. Taxes: *6*
12. Appointment of Attorney: *7*
13. District Employees Not To Benefit: *7*
14. Disputes: *7*
15. Changes: *10*
16 Termination For Convenience Of The District: *10*
17. Recovery Of Debts Owed The District: *14*
18. Retention and Examination Of Records: *14*
19. Non-Discrimination Clause: *14*
20. Definitions: *16*
21. Health And Safety Standards: *16*
22. Appropriation Of Funds: *16*
23. Buy American Act: *16*
24. Service Contract Act of 1965: *17*
25. Cost and Pricing Data: *23*
26. Multiyear Contract: *25*
27. Termination Of Contracts For Certain Crimes And Violations: *25*

1. Covenant Against Contingent Fees:

The Contractor warrants that no person or selling agency has been employed or retained to solicit or secure the contract upon an agreement or understanding for a commission, percentage, brokerage, or contingent fee, excepting bona fide employees or bona fide established commercial or selling agencies maintained by the Contractor for the purpose of securing business. For breach or violation of this warranty, the District will have the right to terminate the contract without liability or in its discretion to deduct from the contract price or consideration or otherwise recover, the full amount of the commission, percentage, brokerage, or contingent fee.

2. Shipping Instructions – Consignment:

Unless otherwise specified in this Invitation for Bids/Request for Proposals, each case, crate, barrel, package, etc., delivered under this contract must be plainly stencil marked or securely tagged, stating the Contractor's name, contract number and delivery address as noted in the contract. In case of carload lots, the Contractor shall tag the car, stating Contractor's name and contract number. Any failure to comply with these instructions will place the material at the Contractor's risk. Deliveries by rail, water, truck or otherwise, must be within the working hours and in ample time to allow for unloading and if necessary, the storing of the materials or supplies before closing time. Deliveries at any other time will not be accepted unless specific arrangements have been previously made with the contact person identified in the contract at the delivery point.

3. Patents:

The Contractor shall hold and save the District, its officers, agents, servants, and employees harmless from liability of any nature or kind, including costs, expenses, for or on account of any patented or unpatented invention, article, process, or appliance, manufactured or used in the performance of this contract, including their use by the District, unless otherwise specifically stipulated in the contract.

4. Quality:

Contractor's workmanship shall be of the highest grade, and all materials provided under this Contract shall be new, of the best quality and grade, and suitable in every respect for the purpose intended.

5. Inspection Of Supplies:

(a) Definition. "Supplies," as used in this clause, includes, but is not limited to raw materials, components, intermediate assemblies, end products, and lots of supplies.

(b) The Contractor shall be responsible for the materials or supplies covered by this contract until they are delivered at the designated point, but the Contractor shall bear all risk on rejected materials or supplies after notification of rejection. Upon the Contractor's failure to cure within ten (10) days after date of notification, the District may return the rejected materials or supplies to the Contractor at the Contractor's risk and expense.

(c) The Contractor shall provide and maintain an inspection system acceptable to the District covering supplies under this contract and shall tender to the District for acceptance only supplies that have been inspected in accordance with the inspection system and have been found by the Contractor to be in conformity with contract requirements. As part of the

system, the Contractor shall prepare records evidencing all inspections made under the system and the outcome. These records shall be kept complete and made available to the District during contract performance and for as long afterwards as the contract requires. The District may perform reviews and evaluations as reasonably necessary to ascertain compliance with this paragraph. These reviews and evaluations shall be conducted in a manner that will not unduly delay the contract work. The right of review, whether exercised or not, does not relieve the Contractor of the obligations under this contract.

(d) The District has the right to inspect and test all supplies called for by the contract, to the extent practicable, at all places and times, including the period of manufacture, and in any event before acceptance. The District will perform inspections and tests in a manner that will not unduly delay the work. The District assumes no contractual obligation to perform any inspection and test for the benefit of the Contractor unless specifically set forth elsewhere in the contract.

(e) If the District performs inspection or test on the premises of the Contractor or subcontractor, the Contractor shall furnish, and shall require subcontractors to furnish, without additional charge, all reasonable facilities and assistance for the safe and convenient performance of these duties. Except as otherwise provided in the contract, the District will bear the expense of District inspections or tests made at other than Contractor's or subcontractor's premises; provided, that in case of rejection, the District will not be liable for any reduction in the value of inspection or test samples.

(1) When supplies are not ready at the time specified by the Contractor for inspection or test, the Contracting Officer may charge to the Contractor the additional cost of inspection or test.

(2) Contracting Officer may also charge the Contractor for any additional cost of inspection or test when prior rejection makes re-inspection or retest

(f) The District has the right either to reject or to require correction of nonconforming supplies. Supplies are nonconforming when they are defective in material or workmanship or otherwise not in conformity with contract requirements. The District may reject nonconforming supplies with or without disposition instructions.

(g) The Contractor shall remove supplies rejected or required to be corrected. However, the Contracting Officer may require or permit correction in place, promptly after notice, by and at the expense of the Contractor. The Contractor shall not tender for acceptance corrected or rejected supplies without disclosing the former rejection or requirement for correction, and when required, shall disclose the corrective action taken.

(h) If the Contractor fails to remove, replace, or correct rejected supplies that are required to be replaced or corrected within ten (10) days, the District may either (1) by contract or otherwise, remove, replace or correct the supplies and charge the cost to the Contractor or (2) terminate the contract for default. Unless the Contractor corrects or replaces the supplies within the delivery schedule, the Contracting Officer may require their delivery and make an equitable price reduction. Failure to agree to a price reduction shall be a dispute.

(i) If this contract provides for the performance of District quality assurance at source, and if requested by the District, the Contractor shall furnish advance notification of the time (i) when Contractor inspection or tests will be performed in accordance with the terms and conditions of the contract, and (ii) when the supplies will be ready for District inspection.

(j) The District request shall specify the period and method of the advance notification and the District representative to whom it shall be furnished. Requests shall not require more than 2 business days of advance notification if the District representative is in residence in the Contractor's plant, nor more than 7 business days in other instances.

(k) The District will accept or reject supplies as promptly as practicable after delivery, unless otherwise provided in the contract. District failure to inspect and accept or reject the supplies shall not relieve the Contractor from responsibility, nor impose liability upon the District, for non-conforming supplies.

(l) Inspections and tests by the District do not relieve the Contractor of responsibility for defects or other failures to meet contract requirements discovered before acceptance. Acceptance shall be conclusive, except for latent defects, fraud, gross mistakes amounting to fraud, or as otherwise provided in the contract.

(m) If acceptance is not conclusive for any of the reasons in subparagraph (l) hereof, the District, in addition to any other rights and remedies provided by law, or under provisions of this contract, shall have the right to require the Contractor (1) at no increase in contract price, to correct or replace the defective or nonconforming supplies at the original point of delivery or at the Contractor's plant at the Contracting Officer's election, and in accordance with a reasonable delivery schedule as may be agreed upon between the Contractor and the Contracting Officer; provided, that the Contracting Officer may require a reduction in contract price if the Contractor fails to meet such delivery schedule, or (2) within a reasonable time after receipt by the Contractor of notice of defects or noncompliance, to repay such portion of the contract as is equitable under the circumstances if the Contracting Officer elects not to require correction or replacement. When supplies are returned to the Contractor, the Contractor shall bear the transportation cost from the original point of delivery to the Contractor's plant and return to the original point when that point is not the Contractor's plant. If the Contractor fails to perform or act as required in (1) or (2) above and does not cure such failure within a period of 10 days (or such longer period as the Contracting Officer may authorize in writing) after receipt of notice from the Contracting Officer specifying such failure, the District will have the right to return the rejected materials at Contractor's risk and expense or contract or otherwise to replace or correct such supplies and charge to the Contractor the cost occasioned the District thereby.

6. <u>Inspection Of Services:</u>

(a) Definition. "Services" as used in this clause includes services performed, workmanship, and material furnished or utilized in the performance of services.

(b) The Contractor shall provide and maintain an inspection system acceptable to the District covering the services under this contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the District during contract performance and for as long afterwards as the contract requires.

(c) The District has the right to inspect and test all services called for by the contract, to the extent practicable at all times and places during the term of the contract. The District will perform inspections and tests in a manner that will not unduly delay the work.

(d) If the District performs inspections or tests on the premises of the Contractor or subcontractor, the Contractor shall furnish, without additional charge, all reasonable facilities and assistance for the safety and convenient performance of these duties.

(e) If any of the services do not conform to the contract requirements, the District may require the Contractor to perform these services again in conformity with contract requirements, at no increase in contract amount. When the defects in services cannot be corrected by performance, the District may require the Contractor to take necessary action to ensure that future performance conforms to contract requirements and reduce the contract price to reflect value of services performed.

(f) If the Contractor fails to promptly perform the services again or take the necessary action to ensure future performance in conformity to contract requirements, the District may (1) by contract or otherwise, perform the services and charge the Contractor any cost incurred by the District that is directly related to the performance of such services, or (2) terminate the contract for default.

7. <u>Waiver:</u>

The waiver of any breach of the contract will not constitute a waiver of any subsequent breach thereof, or a waiver of the contract.

8. <u>Default:</u>

(a) The District may, subject to the provisions of paragraph (c) below, by written notice of default to the Contractor, terminate the whole or any part of this contract in any one of the following circumstances:

(1) If the Contractor fails to make delivery of the supplies or to perform the services within the time specified herein or any extension thereof; or

(2) If the Contractor fails to perform any of the other provisions of this contract, or so fails to make progress as to endanger performance of this contract in accordance with its terms, and in either of these two circumstances does not cure such failure within a period of ten (10) days (or such longer period as the Contracting Officer may authorize in writing) after receipt of notice from the Contracting Officer specifying such failure.

(b) In the event the District terminates this contract in whole or in part as provided in paragraph (a) of this clause, the District may procure, upon such terms and in such manner as the Contracting Officer may deem appropriate, supplies or service similar to those so terminated, and the Contractor shall be liable to the District for any excess costs for similar supplies or services; provided, that the Contractor shall continue the performance of this contract to the extent not terminated under the provisions of this clause.

(c) Except with respect to defaults of subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the contract arises out of causes beyond the control and without the fault or negligence of the Contractor. Such causes may include, but are not restricted to, acts of God or of the public enemy, acts of the District or Federal Government in either their sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the failure to perform must be beyond the control and without fault or negligence of the Contractor. If the failure to perform is caused by the default of the subcontractor, and if such default arises out of causes beyond the control of both the Contractor and the subcontractor, and without the fault or negligence of either of them, the Contractor shall not be liable for any excess cost for failure to perform, unless the supplies or services to be furnished by the subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required delivery schedule.

(d) If this contract is terminated as provided in paragraph (a) of this clause, the District, in addition to any other rights provided in this clause, may require the Contractor to transfer title and deliver to the District, in the manner and to the extent directed by the Contracting Officer, (i) completed supplies, and (ii) such partially completed supplies and materials, parts, tools, dies, jigs, fixtures plans, drawing information, and contract rights (hereinafter called "manufacturing materials") as the Contractor has specifically produced or specifically acquired for the performance of such part of this contract as has been terminated; and the Contractor shall, upon direction of the Contracting Officer, protect and preserve property in possession of the Contractor in which the District has an interest. Payment for completed supplies delivered to and accepted by the District will be at the contract price. Payment for manufacturing materials delivered to and accepted by the District will be at the contract price. Payment for manufacturing materials delivered to and accepted by the District and for the protection and preservation of property shall be in an amount agreed upon by the Contractor and Contracting Officer; failure to agree to such amount shall be a dispute concerning a question of fact within the meaning of the clause of this contract entitled "Disputes". The District may withhold from amounts otherwise due the Contractor for such completed supplies or manufacturing materials such sum as the Contracting Officer determines to be necessary to protect the District against loss because of outstanding liens or claims of former lien holders.

(e) If, after notice of termination of this contract under the provisions of this clause, it is determined for any reason that the Contractor was not in default under the provisions of this clause, or that the default was excusable under the provisions of this clause, the rights and obligations of the parties shall, if the contract contains a clause providing for termination of convenience of the District, be the same as if the notice of termination had been issued pursuant to such clause. See Clause 20 for Termination for Convenience of the District.

(f) The rights and remedies of the District provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under this contract.

(g) As used in paragraph (c) of this clause, the terms "subcontractor(s) means subcontractor(s) at any tier.

9. Indemnification:

The Contractor agrees to defend, indemnify and hold harmless the District, its officers, agencies, departments, agents, and employees (collectively the "District") from and against any and all claims, losses, liabilities, penalties, fines, forfeitures, demands, causes of action, suits, costs and expenses incidental thereto (including cost of defense and attorneys' fees), resulting from, arising out of, or in any way connected to activities or work performed by the Contractor, Contractor's officers, employees, agents, servants, subcontractors, or any other person acting for or by permission of the Contractor in performance of this Contract. The Contractor assumes all risks for direct and indirect damage or injury to the property or persons used or employed in performance of this Contract. The Contractor shall also repair or replace any District property that is damaged by the Contractor, Contractor's officers, employees, agents, servants, subcontractors, or any other person acting for or by permission of the Contractor while performing work hereunder.

The indemnification obligation under this section shall not be limited by the existence of any insurance policy or by any limitation on the amount or type of damages, compensation or benefits payable by or for Contractor or any subcontractor, and shall survive the termination of this Contract. The District agrees to give Contractor written notice of any claim of indemnity under this section. Additionally, Contractor shall have the right and sole authority to control the defense or settlement of such claim, provided that no contribution or action by the District is required in connection with the settlement. Monies due or to become due the Contractor under the contract may be retained by the District as necessary to satisfy any outstanding claim which the District may have against the Contractor.

10. Transfer:

No contract or any interest therein shall be transferred by the parties to whom the award is made; such transfer will be null and void and will be cause to annul the contract.

11. Taxes:

(a) The Government of the District of Columbia is exempt from and will not pay Federal Excise Tax, Transportation Tax, and the District of Columbia Sales and Use Taxes.

(b) Tax exemption certificates are no longer issued by the District for Federal Excise Tax. The following statement may be used by the supplier when claiming tax deductions for Federal Excise Tax exempt items sold to the District.

"The District of Columbia Government is Exempt from Federal Excise Tax – Registration No. 52-73-0206-K, Internal Revenue Service, Baltimore, Maryland."

Exempt From Maryland Sales Tax, Registered With The Comptroller Of The Treasury As Follows:

a) Deliveries to Glenn Dale Hospital – Exemption No. 4647

b) Deliveries to Children's Center – Exemption No. 4648

c) Deliveries to other District Departments or Agencies – Exemption No. 09339

"The District of Columbia Government is Exempt from Sales and Use Tax – Registration No. 53-600, The District of Columbia Office of Tax and Revenue."

12. Appointment of Attorney:

(a) The bidder/offeror or contractor (whichever the case may be) does hereby irrevocably designate and appoint the Clerk of the District of Columbia Superior Court and his successor in office as the true and lawful attorney of the Contractor for the purpose of receiving service of all notices and processes issued by any court in the District of Columbia, as well as service of all pleadings and other papers, in relation to any action or legal proceeding arising out of or pertaining to this contract or the work required or performed hereunder.

(b) The bidder/offeror or contractor (whichever the case may be) expressly agrees that the validity of any service upon the said Clerk as herein authorized shall not be affected either by the fact that the contractor was personally within the District of Columbia and otherwise subject to personal service at the time of such service upon the said Clerk or by the fact that the contractor failed to receive a copy of such process, notice or other paper so served upon the said Clerk provided the said Clerk shall have deposited in the United States mail, registered and postage prepaid, a copy of such process, notice, pleading or other paper addressed to the bidder/offeror or contractor at the address stated in this contract.

13. District Employees Not To Benefit:

Unless a determination is made as provided herein, no officer or employee of the District will be admitted to any share or part of this contract or to any benefit that may arise therefrom, and any contract made by the Contracting Officer or any District employee authorized to execute contracts in which they or an employee of the District will be personally interested shall be void, and no payment shall be made thereon by the District or any officer thereof, but this provision shall not be construed to extend to this contract if made with a corporation for its general benefit. A District employee shall not be a party to a contract with the District and will not knowingly cause or allow a business concern or other organization owned or substantially owned or controlled by the employee to be a party to such a contract, unless a written determination has been made by the head of the procuring agency that there is a compelling reason for contracting with the employee, such as when the District's needs cannot reasonably otherwise be met. (DC Procurement Practices Act of 1985, D.C. Law 6-85, D.C. Official Code, section 2-310.01, and Chapter 18 of the DC Personnel Regulations)

The Contractor represents and covenants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of its services hereunder. The Contractor further covenants not to employ any person having such known interests in the performance of the contract.

14. Disputes:

A. All disputes arising under or relating to this contract shall be resolved as provided herein.

B. Claims by a Contractor against the District.

Claim, as used in Section B of this clause, means a written assertion by the Contractor seeking, as a matter of right, the payment of money in a sum certain, the adjustment or interpretation of contract terms, or other relief arising under or relating to this contract. A claim arising under a contract, unlike a claim relating to that

contract, is a claim that can be resolved under a contract clause that provides for the relief sought by the claimant.

(a) All claims by a Contractor against the District arising under or relating to a contract shall be in writing and shall be submitted to the Contracting Officer for a decision. The contractor's claim shall contain at least the following:

(1) A description of the claim and the amount in dispute;

(2) Any data or other information in support of the claim;

(3) A brief description of the Contractor's efforts to resolve the dispute prior to filing the claim; and

(4) The Contractor's request for relief or other action by the Contracting Officer.

(b) The Contracting Officer may meet with the Contractor in a further attempt to resolve the claim by agreement.

(c) For any claim of $50,000 or less, the Contracting Officer shall issue a decision within sixty (60) days from receipt of a written request from a Contractor that a decision be rendered within that period.

(d) For any claim over $50,000, the Contracting Officer shall issue a decision within ninety (90) days of receipt of the claim. Whenever possible, the Contracting Officer shall take into account factors such as the size and complexity of the claim and the adequacy of the information in support of the claim provided by the Contractor.

(e) The Contracting Officer's written decision shall do the following:

(1) Provide a description of the claim or dispute;

(2) Refer to the pertinent contract terms;

(3) State the factual areas of agreement and disagreement;

(4) State the reasons for the decision, including any specific findings of fact, although specific findings of fact are not required and, if made, shall not be binding in any subsequent proceeding;

(5) If all or any part of the claim is determined to be valid, determine the amount of monetary settlement, the contract adjustment to be made, or other relief to be granted;

(6) Indicate that the written document is the contracting officer's final decision; and

(7) Inform the Contractor of the right to seek further redress by appealing the decision to the Contract Appeals Board.

(f) Any failure by the Contracting Officer to issue a decision on a contract claim within the required time period will be deemed to be a denial of the claim, and will authorize the commencement of an appeal to the Contract Appeals Board as authorized by D.C. Official Code § 2-309.04.

(g) (1) If a Contractor is unable to support any part of his or her claim and it is determined that the inability is attributable to a material misrepresentation of fact or fraud on the part of the Contractor, the Contractor shall be liable to the District for an amount equal to the unsupported part of the claim in addition to all costs to the District attributable to the cost of reviewing that part of the Contractor's claim.

(2) Liability under paragraph (g)(1) shall be determined within six (6) years of the commission of the misrepresentation of fact or fraud.

(h) The decision of the Contracting Officer shall be final and not subject to review unless an administrative appeal or action for judicial review is timely commenced by the Contractor as authorized by D. C. Official Code § 2-309.04.

(i) Pending final decision of an appeal, action, or final settlement, a Contractor shall proceed diligently with performance of the contract in accordance with the decision of the Contracting Officer.

C. Claims by the District against a Contractor

(a) Claim as used in Section C of this clause, means a written demand or written assertion by the District seeking, as a matter of right, the payment of money in a sum certain, the adjustment of contract terms, or other relief arising under or relating to this contract. A claim arising under a contract, unlike a claim relating to that contract, is a claim that can be resolved under a contract clause that provides for the relief sought by the claimant.

(b) (1) All claims by the District against a Contractor arising under or relating to a contract shall be decided by the Contracting Officer.

(2) The Contracting Officer shall send written notice of the claim to the Contractor. The Contracting Officer's written decision shall do the following:

(a) Provide a description of the claim or dispute;

(b) Refer to the pertinent contract terms;

(c) State the factual areas of agreement and disagreement;

(d) State the reasons for the decision, including any specific findings of fact, although specific findings of fact are not required and, if made, shall not be binding in any subsequent proceeding;

(e) If all or any part of the claim is determined to be valid, determine the amount of monetary settlement, the contract adjustment to be made, or other relief to be granted;

(f) Indicate that the written document is the Contracting Officer's final decision; and

(g) Inform the Contractor of the right to seek further redress by appealing the decision to the Contract Appeals Board.

(3) The decision shall be supported by reasons and shall inform the Contractor of its rights as provided herein.

(4) The authority contained in this clause shall not apply to a claim or dispute for penalties or forfeitures prescribed by statute or regulation which another District agency is specifically authorized to administer, settle, or determine.

(5) This clause shall not authorize the Contracting Officer to settle, compromise, pay, or otherwise adjust any claim involving fraud.

(c) The decision of the Contracting Officer shall be final and not subject to review unless an administrative appeal or action for judicial review is timely commenced by the Contractor as authorized by D.C. Official Code §2-309.04.

(d) Pending final decision of an appeal, action, or final settlement, the Contractor shall proceed diligently with performance of the contract in accordance with the decision of the Contracting Officer.

15. Changes:

The Contracting Officer may, at any time, by written order, and without notice to the surety, if any, make changes in the contract within the general scope hereof. If such change causes an increase or decrease in the cost of performance of this contract, or in the time required for performance, an equitable adjustment shall be made. Any claim for adjustment under this paragraph must be asserted within ten (10) days from the date the change is offered; provided, however, that the Contracting Officer, if he or she determines that the facts justify such action, may receive, consider and adjust any such claim asserted at any time prior to the date of final settlement of the contract. If the parties fail to agree upon the adjustment to be made, the dispute shall be determined as provided in the Disputes clause at Section 18. Nothing in this clause shall excuse the Contractor from proceeding with the contract as changed.

16. Termination For Convenience Of The District:

(a) The District may terminate performance of work under this contract in whole or, from time to time, in part if the Contracting Officer determines that a termination is in the District's interest. The Contracting Officer shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and effective date.

(b) After receipt of a Notice of Termination, and except as directed by the Contracting Officer, the Contractor shall immediately proceed with the following obligations, regardless of any delay in determining or adjusting any amounts due under this clause:

(1) Stop work as specified in the notice.

(2) Place no further subcontracts or orders (referred to as subcontracts in this clause) for materials, services, or facilities, except as necessary to complete the continued portion of the contract.

(3) Terminate all contracts to the extent they relate to the work terminated.

(4) Assign to the District, as directed by the Contracting Officer, all rights, title and interest of the Contractor under the subcontracts terminated, in which case the District will have the right to settle or pay any termination settlement proposal arising out of those terminations.

(5) With approval or ratification to the extent required by the Contracting Officer, settle all outstanding liabilities and termination settlement proposals arising from the termination of subcontracts. The approval or ratification will be final for purposes of this clause.

(6) As directed by the Contracting Officer, transfer title and deliver to the District (i) the fabricated or unfabricated parts, work in process, completed work, supplies, and other materials produced or acquired for the work terminated, and (ii) the completed or partially completed plans, drawings, information, and other property that, if the contract has been completed, would be required to be furnished to the District.

(7) Complete performance of the work not terminated.

(8) Take any action that may be necessary, or that the Contracting Officer may direct, for the protection and preservation of the property related to this contract that is in the possession of the Contractor and in which the District has or may acquire an interest.

(9) Use its best efforts to sell, as directed or authorized by the Contracting Officer, any property of the types referred to in subparagraph (6) above; provided, however, that the Contractor (i) is not required to extend credit to any purchaser and (ii) may acquire the property under the conditions prescribed by, and at prices approved by, the Contracting Officer. The proceeds of any transfer or disposition will be applied to reduce any payments to be made by the District under this contract, credited to the price or cost of the work, or paid in any other manner directed by the Contracting Officer.

(c) After the expiration of ninety (90) days (or such longer period as may be agreed to) after receipt by the Contracting Officer of acceptable inventory schedules, the Contractor may submit to the Contracting Officer a list, certified as to quantity and quality of termination inventory not previously disposed of excluding items authorized for disposition by the Contracting Officer. The Contractor may request the District to remove those items or enter into an agreement for their storage. Within fifteen (15) days, the District will accept title to those items and remove them or enter into a storage agreement. The Contracting Officer may verify the list upon removal of the items, or if stored, within forty five (45) days from submission of the list, and shall correct the list, as necessary, before final settlement.

(d) After termination, the Contractor shall submit a final termination settlement proposal to the Contracting Officer in the form and with the certification prescribed by the Contracting Officer. The Contractor shall submit the proposal promptly, but no later than one year from the effective date of termination, unless extended in writing by the Contracting Officer upon written request of the Contractor within this one year period. However, if the Contracting Officer determines that the facts justify it, a termination settlement proposal may be

received and acted on after one year or any extension. If the Contractor fails to submit the proposal within the time allowed, the Contracting Officer may determine, on the basis of information available, the amount, if any, due to the Contractor because of the termination and shall pay the amount determined.

(e) Subject to paragraph (d) above, the Contractor and the Contracting Officer may agree upon the whole or any part of the amount to be paid because of the termination. The amount may include a reasonable allowance for profit on work done. However, the agreed amount, whether under this paragraph (e) or paragraph (f) below, exclusive of costs shown in subparagraph (f)(3) below, may not exceed the total contract price as reduced by (1) the amount of payment previously made and (2) the contract price of work not terminated. The contract shall be amended, and the Contractor paid the agreed amount. Paragraph (f) below shall not limit, restrict, or affect the amount that may be agreed upon to be paid under this paragraph.

(f) If the Contractor and the Contracting Officer fail to agree on the whole amount to be paid because of the termination work, the Contracting Officer shall pay the Contractor the amounts determined by the Contracting Officer as follows, but without duplication of any amounts agreed on under paragraph (e) above:

(1) The contract price for completed supplies or services accepted by the District (or sold or acquired under subparagraph (b)(9) above) not previously paid for, adjusted for any saving of freight and other charges.

(2) The total of :

(i) The costs incurred in the performance of the work terminated, including initial costs and preparatory expense allocable thereto, but excluding any costs attributable to supplies or services paid or to be paid under subparagraph (f)(1) above;

(ii) The cost of settling and paying termination settlement proposals under terminated subcontracts that are properly chargeable to the terminated portion of the contract if not included in subparagraph (f)(1) above; and

(iii) A sum, as profit on subparagraph f(1) above, determined by the Contracting Officer to be fair and reasonable; however, if it appears that the Contractor would have sustained a loss on the entire contract had it been completed, the Contracting Officer shall allow no profit under this subparagraph (iii) and shall reduce the settlement to reflect the indicated rate of loss.

(3) The reasonable cost of settlement of the work terminated, including-

(i) Accounting, legal, clerical, and other expenses reasonably necessary for the preparation of termination settlement proposals and supporting data;

(ii) The termination and settlement of subcontractors (excluding the amounts of such settlements); and

(iii) Storage, transportation, and other costs incurred, reasonably necessary for the preservation, protection, or disposition of the termination inventory.

(g) Except for normal spoilage, and except to the extent that the District expressly assumed the risk of loss, the Contracting Officer shall exclude from the amounts payable to the Contractor under paragraph (f) above, the fair value as determined by the Contracting Officer, of property that is destroyed, lost, stolen, or damaged so as to become undeliverable to the District or to a buyer.

(h) The Contractor shall have the right of appeal, under the Disputes clause, from any determination made by the Contracting Officer under paragraphs (d), (f) or (j), except that if the Contractor failed to submit the termination settlement proposal within the time provided in paragraph (d) or (j), and failed to request a time extension, there is no right of appeal. If the Contracting Officer has made a determination of the amount due under paragraph (d), (f) or (j), the District will pay the Contractor (1) the amount determined by the Contracting Officer if there is no right of appeal or if no timely appeal has been taken, or (2) the amount finally determined on an appeal.

(i) In arriving at the amount due the Contractor under this clause, there shall be deducted:

(1) All unliquidated advances or other payments to the Contractor under the termination portion of the contract;

(2) Any claim which the District has against the Contractor under this contract; and

(3) The agreed price for, or the proceeds of sale of, materials, supplies, or other things acquired by the Contractor or sold under the provisions of this clause and not recovered by or credited to the District.

(j) If the termination is partial, the Contractor may file a proposal with the Contracting Officer for an equitable adjustment of the price(s) of the continued portion of the contract. The Contracting Officer shall make any equitable adjustment agreed upon. Any proposal by the Contractor for an equitable adjustment under this clause shall be requested within ninety (90) days from the effective date of termination unless extended in writing by the Contracting Officer.

(k) (1) The District may, under the terms and conditions it prescribes, make partial payments and payments against costs incurred by the Contractor for the terminated portion of the contract, if the Contracting Officer believes the total of these payments will not exceed the amount to which the Contractor shall be entitled.

(2) If the total payments exceed the amount finally determined to be due, the Contractor shall repay the excess to the District upon demand together with interest computed at the rate of 10 percent (10%) per year. Interest shall be computed for the period from the date the excess payment is received by the Contractor to the date the excess payment is repaid. Interest shall not be charged on any excess payment due to a reduction in the Contractor's termination settlement proposal because of retention or

other disposition of termination inventory until 10 days after the date of the retention or disposition, or a later date determined by the Contracting Officer because of the circumstances.

(l) Unless otherwise provided in this contract or by statute, the Contractor shall maintain all records and documents relating to the terminated portion of this contract for 3 years after final settlement. This includes all books and other evidence bearing on the Contractor's costs and expenses under this contract. The Contractor shall make these records and documents available to the District, at the Contractor's office, at all reasonable times, without any direct charge. If approved by the Contracting Officer, photographs, micrographs, or other authentic reproductions may be maintained instead of original records and documents.

17. Recovery Of Debts Owed The District:

The Contractor hereby agrees that the District may use all or any portion of any consideration or refund due the Contractor under the present contract to satisfy, in whole or part, any debt due the District.

18. Retention and Examination Of Records:

The Contractor shall establish and maintain books, records, and documents (including electronic storage media) in accordance with generally accepted accounting principles and practices which sufficiently and properly reflect all revenues and expenditures of funds provided by the District under the contract that results from this solicitation.

The Contractor shall retain all records, financial records, supporting documents, statistical records, and any other documents (including electronic storage media) pertinent to the contract for a period of three (3) years after termination of the contract, or if an audit has been initiated and audit findings have not been resolved at the end of three (3) years, the records shall be retained until resolution of the audit findings or any litigation which may be based on the terms of the contract.

The Contractor shall assure that these records shall be subject at all reasonable times to inspection, review, or audit by Federal, District, or other personnel duly authorized by the Contracting Officer.

The Contracting Officer, the Inspector General and the District of Columbia Auditor, or any of their duly authorized representatives shall, until three years after final payment, have the right to examine any directly pertinent books, documents, papers and records of the Contractor involving transactions related to the contract.

19. Non-Discrimination Clause:

(a) The Contractor shall not discriminate in any manner against any employee or applicant for employment that would constitute a violation of the District of Columbia Human Rights Act, approved December 13, 1977, as amended (D. C. Law 2-38; D. C. Official Code §2-1402.11) (2001 Ed.)("Act" as used in this Section). The Contractor shall include a similar clause in all subcontracts, except subcontracts for standard commercial supplies or raw materials. In addition, Contractor agrees and any subcontractor shall agree to post in conspicuous places, available to employees and applicants for employment, notice setting forth the provisions of this non-discrimination clause as provided in Section 251 of the Act.

(b) Pursuant to rules of the Office of Human Rights, published on August 15, 1986 in the D. C. Register, Mayor's Order 2002-175 (10/23/02), 49 DCR 9883 and Mayor's Order 2006-151 (11/17/06), 52 DCR 9351, the following clauses apply to this contract:

(1) The Contractor shall not discriminate against any employee or applicant for employment because of actual or perceived: race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, disability, matriculation, political affiliation, genetic information, source of income, or place of residence or business. Sexual harassment is a form of sex discrimination which is prohibited by the Act. In addition, harassment based on any of the above protected categories is prohibited by the Act.

(2) The Contractor agrees to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their actual or perceived: race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, disability, matriculation, political affiliation, genetic information, source of income, or place of residence or business.

The affirmative action shall include, but not be limited to the following:

(a) employment, upgrading or transfer;

(b) recruitment, or recruitment advertising;

(c) demotion, layoff, or termination;

(d) rates of pay, or other forms of compensation; and

(e) selection for training and apprenticeship.

(3) The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Contracting Agency, setting forth the provisions in subsections (b)(1) and (b)(2) concerning non-discrimination and affirmative action.

(4) The Contractor shall, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment pursuant to the non-discrimination requirements set forth in subsection (b)(2).

(5) The Contractor agrees to send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided by the contracting agency, advising the said labor union or workers' representative of that contractor's commitments under this nondiscrimination clause and the Act, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(6) The Contractor agrees to permit access to his books, records and accounts pertaining to its employment practices, by the Chief Procurement Officer or designee, or the Director of Human Rights or designee, for purposes of investigation to ascertain compliance with this chapter, and to require under terms of any subcontractor agreement each subcontractor to permit access of such subcontractors' books, records, and accounts for such purposes.

(7) The Contractor agrees to comply with the provisions of this chapter and with all guidelines for equal employment opportunity applicable in the District of Columbia adopted by the Director of the Office of Human Rights, or any authorized official.

(8) The Contractor shall include in every subcontract the equal opportunity clauses, subsections (b)(1) through (b)(9) of this section, so that such provisions shall be binding upon each subcontractor or vendor.

(9) The Contractor shall take such action with respect to any subcontract as the Contracting Officer may direct as a means of enforcing these provisions, including sanctions for noncompliance; provided, however, that in the event the Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the contracting agency, the Contractor may request the District to enter into such litigation to protect the interest of the District.

20. <u>Definitions:</u>

The terms Mayor, Chief Procurement Officer, Contract Appeals Board and District will mean the Mayor of the District of Columbia, the Chief Procurement Officer of the District of Columbia or his/her alternate, the Contract Appeals Board of the District of Columbia, and the Government of the District of Columbia respectively. If the Contractor is an individual, the term Contractor shall mean the Contractor, his heirs, his executor and his administrator. If the Contractor is a corporation, the term Contractor shall mean the Contractor and its successor.

21. <u>Health And Safety Standards:</u>

Items delivered under this contract shall conform to all requirements of the Occupational Safety and Health Act of 1970, as amended ("OSHA"), and Department of Labor Regulations under OSHA, and all Federal requirements in effect at time of bid opening/proposal submission.

22. <u>Appropriation Of Funds:</u>

The District's liability under this contract is contingent upon the future availability of appropriated monies with which to make payment for the contract purposes. The legal liability on the part of the District for the payment of any money shall not arise unless and until such appropriation shall have been provided.

23. <u>Buy American Act:</u>

(a) The Buy American Act (41 U.S.C. §10a) provides that the District give preference to domestic end products.

"Components," as used in this clause, means those articles, materials, and supplies incorporated directly into the end products.

"Domestic end product," as used in this clause, means, (1) an unmanufactured end product mined or produced in the United States, or (2) an end product manufactured in the United States, if the cost of its components mined, produced, or manufactured in the United States, exceeds 50 percent of the cost of all its components. Components of foreign origin of the same class or kind as the products referred to in paragraphs (b)(2) or (3) of this clause shall be treated as domestic. Scrap generated, collected, and prepared for processing in the United States is considered domestic.

"End products," as used in this clause, means those articles, materials, and supplies to be acquired for public use under this contract.

(b) The Contractor shall deliver only domestic end products, except those-

(1) For use outside the United States;

(2) That the District determines are not mined, produced, or manufactured in the United States in sufficient and reasonably available commercial quantities of a satisfactory quality;

(3) For which the District determines that domestic preference would be inconsistent with the public interest; or

(4) For which the District determines the cost to be unreasonable.

24. <u>Service Contract Act of 1965:</u>

(a) <u>Definitions.</u> "Act," as used in this clause, means the Service Contract Act of 1965, as amended (41 U.S.C. §351, *et seq.).*

(1) "Contractor," as used in this clause, means the prime Contractor or any subcontractor at any tier.

(2) "Service employee," as used in this clause, means any person (other than a person employed in a bona fide executive, administrative, or professional capacity as defined in 29 CFR 541) engaged in performing a District contract not exempted under 41 U.S.C. §356, the principal purpose of which is to furnish services in the United States, as defined in section 22.1001 of the Federal Acquisition Regulation. It includes all such persons regardless of the actual or alleged contractual relationship between them and a contractor.

(b) <u>Applicability.</u> To the extent that the Act applies, this contract is subject to the following provisions and to all other applicable provisions of the Act and regulations of the Secretary of Labor (20 CFR part 4). All interpretations of the Act in Subpart C of 29 CFR 4 are incorporated in this contract by reference. This clause does not apply to contracts or subcontracts administratively exempted by the Secretary of Labor or exempted by 41 U.S.C. §356, as interpreted in Subpart C of 29 CFR 4.

(c) <u>Compensation</u>.

(1) Each service employee employed in the performance of this contract by the Contractor or any subcontractor shall be paid not less than the minimum monetary wages and shall be furnished fringe benefits in accordance with the wages and fringe benefits determined by the Secretary of Labor or the Secretary's authorized representative, as specified in any wage determination attached to this contract.

(2) If a wage determination is attached to this contract, the Contractor shall classify any class of service employees not listed in it, but to be employed under this contract (i.e., the work to be performed is not performed by any classification listed in the wage determination) so as to provide a reasonable relationship (i.e., appropriate level of skill comparison) between such unlisted classifications and the classifications listed in the wage determination. Such conformed class of employees shall be paid the monetary wages and furnished the fringe benefits as are determined pursuant to the procedures in this paragraph. This conforming procedure shall be initiated by the Contractor prior to the performance of contract work by the unlisted class of employee.

(a) The Contractor shall submit Standard Form (SF) 1444, Request for Authorization of Additional Classification and Rate, to the Contracting Officer no later than 30 days after the unlisted class of employee performs any contract work. The Contracting Officer shall review the proposed classification and rate and promptly submit the completed SF 1444 (which must include information regarding the agreement or disagreement of the employees' authorized representatives or the employees themselves together with the agency recommendation), and all pertinent information to the Wage and Hour Division, Employment Standards Administration (ESA), Department of Labor. The Wage and Hour Division will approve, modify, or disapprove the action or render a final determination in the event of disagreement within 30 days of receipt or will notify the Contracting Officer within 30 days of receipt that additional time is necessary;

(b) The final determination of the conformance action by the Wage and Hour Division shall be transmitted to the Contracting Officer who shall promptly notify the Contractor of the action taken. Each affected employee shall be furnished by the Contracting Officer with a written copy of such determination or it shall be posted as a part of the wage determination;

(c) The process of establishing wage and fringe benefit rates that bear a reasonable relationship to those listed in a wage determination cannot be reduced to any single formula. The approach used may vary from wage determination to wage determination depending on the circumstances. Standard wage and salary administration practices which rank various job classifications by pay grade pursuant to point schemes or other job factors may, for example, be relied upon. Guidance may also be obtained from the way different jobs are rated under Federal pay systems (Federal Wage Board Pay System and the General

Schedule) or from other wage determinations issued in the same locality. Basic to the establishment of any conformable wage rate(s) is the concept that a pay relationship should be maintained between job classifications based on the skill required and the duties performed;

(d) In the case of a contract modification, an exercise of an option, or extension of an existing contract, or in any other case where a Contractor succeeds to a contract under which the classification in question was previously conformed pursuant to this clause, a new conformed wage rate and fringe benefits may be assigned to the conformed classification by indexing (*i.e*., adjusting) the previous conformed rate and fringe benefits by an amount equal to the average (mean) percentage increase (or decrease, where appropriate) between the wages and fringe benefits specified for all classifications to be used on the contract which are listed in the current wage determination, and those specified for the corresponding classifications in the previously applicable wage determination. Where conforming actions are accomplished in accordance with this paragraph prior to the performance of contract work by the unlisted class of employees, the Contractor shall advise the Contracting Officer of the action taken but the other procedures in this clause need not be followed;

(e) No employee engaged in performing work on this contract shall in any event be paid less than the currently applicable minimum wage specified under section 6(a)(1) of the Fair Labor Standards Act of 1938, as amended;

(f) The wage rate and fringe benefits finally determined under this clause shall be paid to all employees performing in the classification from the first day on which contract work is performed by them in the classification. Failure to pay the unlisted employees the compensation agreed upon by the interested parties or finally determined by the Wage and Hour Division retroactive to the date such class of employees commenced contract work shall be a violation of the Act and this contract;

(g) Upon discovery of failure to comply with this clause, the Wage and Hour Division shall make a final determination of conformed classification, wage rate, and/or fringe benefits which shall be retroactive to the date such class or classes of employees commenced contract work.

(3) If the term of this contract is more than 1 year, the minimum wages and fringe benefits required for service employees under this contract shall be subject to adjustment after 1 year and not less often than once every 2 years, under wage determinations issued by ESA.

(4) The Contractor can discharge the obligation to furnish fringe benefits specified in the attachment or determined under paragraph (2) of this clause by furnishing any equivalent combinations of bona fide fringe

benefits, or by making equivalent or differential cash payments, in accordance with Subpart B and C of 29 CFR 4.

(d) Minimum wage: In the absence of a minimum wage attachment for this contract, the Contractor shall not pay any service or other employees performing this contract less than the minimum wage specified by section 6(a)(1) of the Fair Labor Standards Act of 1938, as amended (29 U.S.C. §206). Nothing in this clause shall relieve the Contractor of any other legal or contractual obligation to pay a higher wage to any employee.

(e) Successor contracts: If this contract succeeds a contract subject to the Act under which substantially the same services were furnished and service employees were paid wages and fringe benefits provided for in a collective bargaining agreement, then, in the absence of a minimum wage attachment to this contract, the Contractor may not pay any service employee performing this contract less than the wages and benefits, including those accrued and any prospective increases, provided for under that agreement. No Contractor may be relieved of this obligation unless the limitations of 29 CFR 4.1c(b) apply or unless the Secretary of Labor or the Secretary's authorized representative:

(1) Determines that the agreement under the predecessor was not the result of arms-length negotiations; or

(2) Finds, after a hearing under 29 CFR 4.10, that the wages and benefits provided for by that agreement vary substantially from those prevailing for similar services in the locality or determines, as provided in 29 CFR 4.11, that the collective bargaining agreement applicable to service employees employed under the predecessor contract was not entered into as a result of arm's length negotiations. Where it is found in accordance with the review procedures provided in 29 CFR 4.10 and 4.11 and parts 6 and 8 that some or all of the wages and fringe benefits contained in a predecessor Contractor's collective bargaining agreement are substantially at variance with those which prevail for services of a character similar in the locality, and that the collective bargaining agreement applicable to service employees employed under the predecessor contract was not entered into as a result of arm's length negotiations, the Department will issue a new or revised wage determination setting forth the applicable wage rates and fringe benefits. Such determination shall be made part of the contract or subcontract, in accordance with the decision of the Administrator, the Administrative Law Judge, or the Board of Service Contract Appeals, as the case may be, irrespective of whether such issuance occurs prior to or after the award of a contract or subcontract (53 Comp. Gen. 401 (1973)). In the case of a wage determination issued solely as a result of a finding of substantial variance, such determination shall be effective as of the date of the final administrative decision.

(f) Notification to employees: The Contractor shall notify each service employee commencing work on this contract of a minimum wage and any fringe benefits required to be paid, or shall post a notice of these wages and benefits in a prominent and accessible place at the worksite, using such poster as may be provided by the Department of Labor.

(g) Safe and sanitary working conditions: The Contractor shall not permit services called for by this contract to be performed in buildings or surroundings or under working conditions provided by or under the control or supervision of the Contractor that are unsanitary, hazardous, or dangerous to the health or safety of service employees. The Contractor shall comply with the health standards applied under 29 CFR Part 1925.

(h) Records: The Contractor shall maintain for 3 years from the completion of work, and make available for inspection and transcription by authorized ESA representatives, a record of the following:

(1) For each employee subject to the Act:

(a) Name and address;

(b) Work classification or classifications, rate or rates of wages and fringe benefits provided, rate or rates of payments in lieu of fringe benefits, and total daily and weekly compensation;

(c) Daily and weekly hours worked; and

(d) Any deductions, rebates, or refunds from total daily or weekly compensation.

(2) For those classes of service employees not included in any wage determination attached to this contract, wage rates or fringe benefits determined by the interested parties or by ESA under the terms of paragraph (c)(3) of this clause. A copy of the report required by paragraph (e) of this clause will fulfill this requirement.

(3) Any list of the predecessor Contractor's employees which had been furnished to the Contractor as prescribed by this clause. The Contractor shall also make available a copy of this contract for inspection or transcription by authorized representatives of the Wage and Hour Division. Failure to make and maintain or to make available these records for inspection and transcription shall be a violation of the regulations and this contract, and in the case of failure to produce these records, the Contracting Officer, upon direction of the Department of Labor and notification to the Contractor, shall take action to cause suspension of any further payment or advance of funds until the violation ceases. The Contractor shall permit authorized representatives of the Wage and Hour Division to conduct interviews with employees at the worksite during normal working hours.

(i) Pay periods: The Contractor shall unconditionally pay to each employee subject to the Act all wages due free and clear and without subsequent deduction (except as otherwise provided by law or regulations, 29 CFR part 4), rebate, or kickback on any account. These payments shall be made no later than one pay period following the end of the regular pay period in which the wages were earned or accrued. A pay period under this Act may not be of any duration longer than semi-monthly.

(j) Withholding of payments and termination of contract: The Contracting Officer shall withhold from the prime Contractor under this or any other District contract

with the prime contractor any sums the Contracting Officer, or an appropriate officer of the Labor Department, decides may be necessary to pay underpaid employees. In the event of failure to pay any employees subject to the Act all or part of the wages or fringe benefits due under the Act, the Contracting Officer may, after authorization or by direction of the Department of Labor and written notification to the Contractor, take action to cause suspension of any further payment or advance of funds until such violations have ceased. Additionally, any failure to comply with the requirements of this clause may be grounds for termination for default. In such event, the District may enter into other contracts or arrangements for completion of the work, charging the Contractor in default with any additional cost.

(k) Subcontracts: The Contractor agrees to insert this clause in all subcontracts.

(l) Contractor's report:

(1) If there is a wage determination attachment to this contract and any classes of service employees not listed on it are to be employed under the contract, the Contractor shall report promptly to the Contracting Officer the wages to be paid and the fringe benefits to be provided each of these classes, when determined under paragraph (c) of this clause.

(2) If wages to be paid or fringe benefits to be furnished any service employees under the contract are covered in a collective bargaining agreement effective at any time when the contract is being performed, the Contractor shall provide to the Contracting Officer a copy of the agreement and full information on the application and accrual of wages and benefits (including any prospective increases) to service employees working on the contract. The Contractor shall report when contract performance begins, in the case of agreements then in effect, and shall report subsequently effective agreements, provisions, or amendments promptly after they are negotiated.

(m) Contractor's Certification: By entering into this contract, the Contractor (and officials thereof) certifies that neither it (nor he or she) nor any person or firm who has a substantial interest in the Contractor's firm is a person or firm ineligible to be awarded District contracts by virtue of the sanctions imposed under section 5 of the Act. No part of this contract shall be subcontracted to any person or firm ineligible for award of a District contract under section 5 of the Act. The penalty for making false statements is prescribed in the U.S. Criminal Code, 18 U.S.C. §1001.

(n) Variations, tolerances, and exemptions involving employment: Notwithstanding any of the provisions in paragraphs (c) through (l) of this clause, the following employees may be employed in accordance with the following variations, tolerances, and exemptions authorized by the Secretary of Labor.

(1)(i) In accordance with regulations issued under Section 14 of the Fair Labor Standards Act of 1938 by the Administrator of the Wage and Hour Division, ESA (29 CFR 520, 521, 524, and 525), apprentices, student learners, and workers whose earning capacity is impaired by age or by physical or mental deficiency or injury, may be employed at wages lower than the minimum wages otherwise required by section 2(a)(1) or 2(b)(1)

of the Service Contract Act, without diminishing any fringe benefits or payments in lieu of these benefits required under section 2(a)(2) of the Act.

(ii) The Administrator will issue certificates under the Act for employing apprentices, student-learners, handicapped persons, or handicapped clients of sheltered workshops not subject to the Fair Labor Standards Act of 1938, or subject to different minimum rates of pay under the two acts, authorizing appropriate rates of minimum wages, but without changing requirements concerning fringe benefits or supplementary cash payments in lieu of these benefits.

(iii) The Administrator may also withdraw, annul, or cancel such certificates under 29 CFR 525 and 528.

(2) An employee engaged in an occupation in which the employee customarily and regularly receives more than $30 a month in tips shall be credited by the employer against the minimum wage required by section 2(a)(1) or section 2(b)(1) of the Act, in accordance with regulations in 29 CFR 531. However, the amount of credit shall not exceed 40 percent of the minimum rate specified in section 6(a)(1) of the Fair Labor Standards Act of 1938 as amended.

25. <u>Cost and Pricing Data:</u>

(a) This paragraph and paragraphs b through e below shall apply to contractors or offerors in regards to: (1) any procurement in excess of $100,000, (2) any contract awarded through competitive sealed proposals, (3) any contract awarded through sole source procurement, or (4) any change order or contract modification. By entering into this contract or submitting this offer, the Contractor or offeror certifies that, to the best of the Contractor's or offeror's knowledge and belief, any cost and pricing data submitted was accurate, complete and current as of the date specified in the contract or offer.

(b) Unless otherwise provided in the solicitation, the offeror or Contractor shall, before entering into any contract awarded through competitive sealed proposals or through sole source procurement or before negotiating any price adjustments pursuant to a change order or modification, submit cost or pricing data and certification that, to the best of the Contractor's knowledge and belief, the cost or pricing data submitted was accurate, complete, and current as of the date of award of this contract or as of the date of negotiation of the change order or modification.

(c) If any price, including profit or fee, negotiated in connection with this contract, or any cost reimbursable under this contract, was increased by any significant amount because (1) the Contractor or a subcontractor furnished cost or pricing data that were not complete, accurate, and current as certified by the Contractor, (2) a subcontractor or prospective subcontractor furnished the Contractor cost or pricing data that were not complete, accurate, and current as certified by the Contractor, or (3) any of these parties furnished data of any description that were not accurate, the price or cost shall be reduced accordingly and the contract shall be modified to reflect the reduction.

(d) Any reduction in the contract price under paragraph c above due to defective data from a prospective subcontractor that was not subsequently awarded, the subcontract shall be limited to the amount, plus applicable overhead and profit markup, by which (1) the actual subcontract or (2) the actual cost to the Contractor, if there was no subcontract, was less than the prospective subcontract cost estimate submitted by the Contractor; provided that the actual subcontract price was not itself affected by defective cost or pricing data.

(e) Cost or pricing data includes all facts as of the time of price agreement that prudent buyers and sellers would reasonably expect to affect price negotiations significantly. Cost or pricing data are factual, not judgmental, and are therefore verifiable. While they do not indicate the accuracy of the prospective Contractor' s judgment about estimated future costs or projections, cost or pricing data do include the data forming the basis for that judgment. Cost or pricing data are more than historical accounting data; they are all the facts that can be reasonably expected to contribute to the soundness of estimates of future costs and to the validity of determinations of costs already incurred.

(f) The following specific information should be included as cost or pricing data, as applicable:

(1) Vendor quotations;

(2) Nonrecurring costs;

(3) Information on changes in production methods or purchasing volume;

(4) Data supporting projections of business prospects and objectives and related operations costs;

(5) Unit – cost trends such as those associated with labor efficiency;

(6) Make or buy decisions;

(7) Estimated resources to attain business goals;

(8) Information on management decisions that could have a significant bearing on costs.

(g) If the offeror or contractor is required by law to submit cost or pricing data in connection with pricing this contract or any change order or modification of this contract, the Contracting Officer or representatives of the Contracting Officer shall have the right to examine all books, records, documents and other data of the Contractor (including computations and projections) related to negotiating, pricing, or performing the contract, change order or modification, in order to evaluate the accuracy, completeness, and currency of the cost or pricing data. The right of examination shall extend to all documents necessary to permit adequate evaluation of the cost or pricing data submitted, along with the computations and projections used. Contractor shall make available at its office at all reasonable times the materials described above for examination, audit, or reproduction until three years after the later of:

(1) final payment under the contract;

(2) final termination settlement; or

(3) the final disposition of any appeals under the disputes clause or of litigation or the settlement of claims arising under or relating to the contract.

26. <u>Multiyear Contract:</u>

If this contract is a multiyear contract, then the following provision is made part of this contract:

If funds are not appropriated or otherwise made available for the continued performance in a subsequent year of a multiyear contract, the contract for the subsequent year shall be terminated, either automatically or in accordance with the termination clause of the contract. Unless otherwise provided for in the contract, the effect of termination is to discharge both the District and the Contractor from future performance of the contract, but not from the existing obligations. The Contractor shall be reimbursed for the reasonable value of any non-recurring costs incurred but not amortized in the price of the supplies or services delivered under the contract.

27. <u>Termination Of Contracts For Certain Crimes And Violations:</u>

(a) The District may terminate without liability any contract and may deduct from the contract price or otherwise recover the full amount of any fee, commission, percentage, gift, or consideration paid in violation of this title if:

(1) The Contractor has been convicted of a crime arising out of or in connection with the procurement of any work to be done or any payment to be made under the contract; or

(2) There has been any breach or violation of:

(A) Any provision of the Procurement Practices Act of 1985, as amended, or

(B) The contract provision against contingent fees.

(b) If a contract is terminated pursuant to this section, the Contractor:

(1) May be paid only the actual costs of the work performed to the date of termination, plus termination costs, if any; and

(2) Shall refund all profits or fixed fees realized under the Contract.

(c) The rights and remedies contained in this are in addition to any other right or remedy provided by law, and the exercise of any of them is not a waiver of any other right or remedy provided by law.

Attachment J.6

Hospital _____
Submission Date_____
DHS/IMA Receipt Date_____

NEWBORN NOTIFICATION FORM

REQUEST TO ADD NEWBORNS
TO DC MEDICAID, PUBLIC ASSISTANCE AND FOOD STAMP ROLLS

Mother's Medicaid I.D. Number:_____ Eligibility Period:_____

Mother's Name:_____ Telephone: _____

Mother's Address: _____

_____

Father's Name: _____ Telephone: _____

Newborn's Name: _____ Date of Birth _____

Place of Birth: _____ Sex _____ Date of Birth _____

I hereby request that my child, _____, be added to my Medicaid eligibility case.

This also serves as the official report to D.C. DHS of this birth for Public Assistance and/or Food Stamp Program Purposes. If I am currently receiving these services, I am requesting that my child be added to my PA and/or FS household.

_____
Mother's Signature

_____
Date of Report

I do hereby certify that the above information is as reported by the birth hospital.

_____
Utilization Reviewer

Telephone: _____

_____
MCO Medical Director

Telephone:_____

District of Columbia Healthy Tots and Teen/Health Check Periodicity Schedule

The DC Healthy Tots and Teens/ Health Check Periodicity Schedule follows the American Academy of Pediatrics (AAP) health recommendation in consultation with local medical community. The recommendations are for the care of children who have no manifestation of any important health problems. Additional visits or interperiodic screens may become necessary if circumstances suggest the need for more screens, i.e. medical conditions, referral by parent, Head State, DC Public Schools, Early Intervention Programs. If a child comes under care for the first time at any point on the schedule or if any items are not done at the suggest age, the schedule should then be brought up to date as soon as possible.

	INFANCY									EARLY CHILDHOOD			MIDDLE CHILDHOOD						ADOLESCENCE										
Age	Prenatal	Newborn	2-4d	by 1m	2m	4m	6m	9m	12mo	15mo	18mo	24mo	3y	4y	5y	6y	8y	10y	11y	12y	13y	14y	15y	16y	17y	18y	19y	20y	21y
HISTORY																													
Initial/Interval	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
MEASUREMENTS																													
Height and Weight		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Head Circumference		●	●	●	●	●	●	●	●	●	●	●																	
Blood Pressure													●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
SENSORY SCREENING																													
Vision		S	S	S	S	S	S	S	S	S	S	S	O[6]	S	O	O	O	O	S	O	S	S	O	S	S	O	S	S	S
Hearing		O[7]	S	S	S	S	S	S	S	S	S	S	S	S	O	O	O	O	S	O	S	S	O	S	S	O	S	S	S
DEVELOPMENTAL/BEHAVIORAL ASSESSMENT [8]		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Physical Examination[9]		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Procedures-General [10]																													
Hereditary/Metabolic Screening [11]		◄	●	►																									
Immunization[12]		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Hematocrit or Hemoglobin[13]								●	►	*	*	*	*	*	*	*	*	*	◄		●								►
Urinalysis[14-15]																			◄					●[14]					►
PROCEDURES-PATIENTS AT RISK																													
Lead Screening [16]							*	*	●	*	*	●	*	*	*														
Tuberculin Test[17] (PPD)									●	►				*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Cholesterol Screening[18]													*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
STD Screening[19]																			*	*	*	*	*	*	*	*	*	*	*
Pelvic Exam [20]																			*	*	*	*	*	*	*	*	*	*	*
ANTICIPATORY GUIDANCE[21]	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Injury Prevention[22]	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Violence Prevention[23]	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sleep Positioning Counseling[24]	●	●	●	●	●	●	●																						
Nutrition Counseling [25]	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
DENTAL EVALUATION/REFERRAL									◄	O	►		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

KEY: ● = to be performed * = to be performed for patients at risk S= subjective, by history O = objective, by a standard testing methods

◄ ● ► = the range during which a service may be provided, with the dot indicating the preferred age. ◄ O ► 12m thru 24 m

1. Prenatal visit is recommended for parents who are at high risk, for first-time parents, and for those who request a conference the prenatal visit should include anticipatory guidance, pertinent medical history, and a discussion of benefits of breastfeeding and planned method of feeding per AAP statement "The Prenatal Visit" (1996).
2. Every infant should have a newborn evaluation after birth. Breastfeeding should be encouragement, and instruction as recommended in the AAP statement "Breastfeeding and the Use of Human Milk" (1997).
3. For newborns discharged in less than 48 hours after delivery refer AAP statement "Hospital Stay for Healthy Term Newborn" (1995).
4. Developmental, psychosocial, and chronic disease issues for children and adolescents may require frequent counseling and treatment visits separate from preventive care visits.
5. If a child comes under care for the first time at any point on the schedule, or if any items are not accomplished at the suggested age, the schedule should be brought up to date at the earliest possible time.
6. If the patient is uncooperative, rescreen within 6 months.
7. All newborns should be screened per the AAP Task Force on Newborn and Infant Hearing Loss in the neonate period (birth to 28 days) and again at 6 months through objective assessment: Hearing screening for children greater than 6 months of age, may be screened through subjective assessments, unless the child is at risk for hearing loss or the subjective evaluation indicates a reason for concern.
8. By history and appropriate physical examinations: If suspicious, by specific objective developmental testing. Parenting skills should be fostered at every visit.
9. At each visit, a complete physical examination is essential, with infant totally unclothed, older child undressed and suitably draped.
10. These may be modified, depending upon entry point into schedule and individual need.
11. Metabolic screening (eg thyroid, hemoglobinopathies, PKU, galactosemia) should be done according to state law.
12. Schedule(s) per the Committee on Infectious Diseases, published annually in the January edition of Pediatrics. Every visit should be an opportunity to update and complete a child's immunizations.
13. All menstruating adolescents should be screened annually.
14. Unless otherwise clinically indicated in other ages, a urinalysis should be preformed, per AAP recommendations, on all sexually active adolescents.
15. Conduct dipstick urinalysis for leukocytes annually for sexually active male and female adolescents.
16. For children at risk of lead exposure refer to the statement "Screening for Elevated Blood Levels" (1998). Children must be screened between 6 months and 14 months and again at 24 months of age. A child over 26 months and less than 6 years without a documented result requires at least one documented BLL result.
17. Current DC regulations require one PPD test for all children entering child care or school, whichever comes first. PPD test is also required for all children who are assessed as high risk for exposure.
18. Cholesterol screening for high-risk patients per AAP statement "Cholesterol in Childhood" (1998). If family history cannot be ascertained and other risk factors are present, screening should be at the discretion of the physician.
19. All sexually active patients should be screened for sexually transmitted diseases (STDs). Refer to STD practice guidelines.
20. All sexually active females should have a pelvic examination. A pelvic examination and routine pap smear should be offered as part of preventive health maintenance between the ages of 18 and 21 year.
21. Age-appropriate discussion and counseling should be an integral part of each visit for care per the AAP Guidelines for Health Supervision III (1998).
22. From birth to age 12, refer to the AAP injury prevention program (TIPP@) as described in A Guide to Safety Counseling in Office Practice (1994).
23. Violence prevention and management for all patients per AAP Statement "The Role of the Pediatrician in Youth Violence Prevention in Clinical Practice and the Community Level " (1999).
24. Parent and caregivers should be advised to place healthy infants on their backs when putting them to sleep. Side positioning is a reasonable alternative but carries a slightly higher of SIDS. Consult the AAP statement 'Changing Concepts of Sudden Infant Death Syndrome: Implications for infant Sleeping Environment and Sleep Position" (2000).
25. Age-appropriate nutrition counseling should be an integral part of each visit per the AAP Handbook of Nutrition (1998).
26. Earlier initial dental examination may be appropriate for some children. Subsequent examinations as prescribed by dentist.

Updated 12/27/05

Attachment J.8

Advisory Committee on Immunization Practices (ACIP) Recommendations (Full version available at: http://www.cdc.gov/nip/publications/acip-list.htm

District of Columbia Department of Health
Medical Assistance Administration
Dental Periodicity Schedule

The District of Columbia Department of Health Medical Assistance Administration (DC DOH MAA) Dental Health Periodicity Schedule follows the American Academy of Pediatric Dentistry Periodicity Schedule oral health recommendations in consultation with local medical communities. This schedule is designed for the care of children who have no contributing medical conditions and are developing normally. The DC DOH MAA Dental periodicity schedule will be modified for children with special health care needs or if disease or trauma manifests variations from normal.

Age	**Birth - 12 months**	**12 - 24 months**	**24 months – 3 years**	**3 - 6 years**	**6 - 12 years**	**12 years & Older**
Clinical Oral screening[1]	•	•	•	•		
Assess oral growth and development[2]	•	•	•	•	•	•
Referral for Regular & Periodic Dental care[3]		If at risk	•	•	•	•
Counseling for nonnutritive Habits[4]	•	•	•	•	•	•
Oral hygiene counseling[5]	•	•	•	•	•	•
Dietary Counseling[6] Injury prevention counseling[7]	•	•	•	•	•	•
Fluoride Supplementation[8]		•	•	•	•	•
Radiographic Assessment[9]			•	•	•	•
Pit & Fissure Sealants[10]			•	•	•	•
Assessment & Treatment of Developing Malocclusion				•	•	•
Assessment and Removal of 3rd molars						•
Substance Abuse Counseling					•	•
Anticipatory Guidance[11]	•	•	•	•	•	•

See Footnotes on Back

1. The Primary Care Physician/Pediatrician should perform the first/initial oral health screening following AAP guidelines.
2. An oral assessment can be done by the Primary Care Physician/Pediatrician up to age 3. Every infant should receive an oral health risk assessment from his/her primary health care provider or qualified health care professional by 6 months of age that includes: (1) assessing the patient's risk of developing oral disease using the AAPD Caries-risk assessment tool; (2) providing education on infant oral health; and (3) evaluating and optimizing fluoride exposure.
3. All children should be referred to a dentist for the establishment of a dental home no later than age 3. Children determined by the PCP/Pediatrician to be at risk for dental caries should be referred to a dentist as early as 6 months after the first tooth erupts, or 12 months of age (whichever comes first) for establishment of a dental home. Children at risk are defined as:
    - Children with Special Health Care Needs
    - Children of mothers with a high caries rate
    - Children with demonstrable caries, plaque, demineralization, and or staining
    - Children who sleep with a bottle or breastfeed throughout the night
    - Later-order offspring
    - Children in families of low socioeconomic status

    Once dental care is established with a dental professional, it is recommended and is the right of every child enrolled in Medicaid to see the Dentist every six months.
4. At first discussion of the need for additional sucking: digits vs. pacifiers; then the need to wean from the habit before malocclusion or skeletal dysphasia occurs.
5. For school-aged children and adolescent patients, counsel regarding any existing habits such as fingernail biting, clenching, or bruxism. Counseling is given to parents/guardians/caregivers up to age 2. At age 2, the provider should include the patient/child in the counseling. For children 12 years and older, counseling need only be done with the child/patient if the dentist feels this is appropriate – Otherwise include the parents.
6. At every screening discuss the role of refined carbohydrates, frequency of snacking, etc.
7. Initial discussions should include play objects, pacifiers, and car seats; when learning to walk, include injury prevention. For school-age children and adolescent patients, counsel regarding sports and routine playing.
8. Fluoride supplementation as indicated including a topical fluoride varnish, as indicated by the child's risk for caries and periodontal disease and the water source. (Performed by dental professional only)
9. As per AAPD "Clinical guideline on prescribing dental radiographs." (Performed by dental professional only)
10. For caries-susceptible primary molars, permanent molars, premolars, and anterior teeth with deep pits and/ or fissures; placed as soon as possible after eruption. (Performed by dental professional only)
11. Appropriate oral health discussion and counseling should be an integral part of each visit for care. (Performed by dental professional only)

REFERENCES FOR DENTAL PERIODICITY SCHEDULE

1. American Academy of Pediatrics, "Policy Statement on Oral Health Risk Assessment Timing and Establishment of the Dental Home", Pediatrics, 111(5):1113-16 (2003).
2. *Guide to Children's Dental Care in Medicaid,* U.S. Department of Health & Human Services, Centers for Medicare and Medicaid Services (Oct. 2004)
3. Cruz GG, Rozier RG, and Slade G, "Dental Screening and Referral of Young Children by Pediatric Primary Care Providers," Pediatrics, 114(5):642-52 (Nov. 2004)
4. Scale NS and Casamassimo PS, "Access to dental care for children in the United States: a survey of general practitioners," JADA, 134:1630-1640 (dec. 2003)
5. American Academy of Pediatric Dentistry, *Policy on Use of a Caries-risk Assessment Tool (CAT) for Infants, Children and Adolescents* Originating Council, Council on Clinical Affairs, Adopted 2002

TAX CERTIFICATION AFFIDAVIT

Date _____, 2007

Name of Organization/Entity: _____

Address: _____

Principal Officers: Name Soc. Sec. No. Title

_____
_____
_____

Business Telephone No.:_____
Finance and Revenue Registration No.: _____
Federal Identification No.: _____
DUNS No.: _____ Contract No.:_____
Unemployment Insurance Account No.: _____

I hereby certify that:

1. I have complied with the applicable tax filing and licensing requirements of the District of Columbia.
2. The following information is true and correct concerning tax compliance for the following taxes for the past five (5) years:

		Current	Not Current
District:	Sales and Use	( )	( )
	Employment Withholding	( )	( )
	Hotel Occupancy	( )	( )
	Corporation Franchise	( )	( )
	Unincorporated Franchise	( )	( )
	Personal Property	( )	( )
	Professional License	( )	( )
	Arena/Public Safety Fee	( )	( )
	Vendor Fee	( )	( )

3. If not current, as checked in item 2, I am in compliance with a payment agreement with the Department of Finance and Revenue.
_____ Yes _____ No Attach copy of the Agreement.

If outstanding liabilities exists and no agreement has been made, please attach a listing of all such liabilities.

The Department of Finance and Revenue also requires:

(A) Copies of FR-532 (Notice of Registration) or a copy of an FR-500 (Combined Registration Form)
(B) Copies of canceled checks for the last tax period(s) filed for each tax liability; i.e., sales and use, employer withholding, etc.

The District of Columbia Government is hereby authorized to verify the above information with appropriate Government authorities. Penalty for making false statements is a fine of not more than $1,000.00, imprisonment for not more than one year, or both, as prescribed in D.C. Code Sec. 22-2514. Penalty for false swearing is a fine of not more than $2,500.00, imprisonment for not more than three (3) years, or both, as prescribed in D.C. Code sec. 22-2513.

_____ _____
Signature of Person Authorized to Sign This Document Title

_____
Print Name

Notary: DISTRICT OF COLUMBIA, ss:

Subscribed and sworn before me this _____ day of _____ Month and Year _____
Notary Public

My Commission Expires _____

Attachment J.12

Reserved

ENROLLED ORIGINAL

Codification District of Columbia Official Code

2001 Edition

2004 Fall Supp.

West Group Publisher

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To provide greater access and participation in public services, programs, and activities for residents of the District of Columbia with limited or no-English proficiency by requiring that District government programs, departments, and services assess the need for, and offer, oral language services; provide written translations of documents into any non-English language spoken by a limited or no-English proficient population that constitutes 3% or 500 individuals, whichever is less, of the population served or encountered, or likely to be served or encountered; to ensure that District government programs, departments, and services with major public contact establish and implement a language access plan and designate a language access coordinator; to require that the Office of Human Rights coordinate and supervise District government programs, departments, and services in complying with the provisions of this act and establish the position of Language Access Director for this purpose; and to amend the District of Columbia Latino Community Development Act and to repeal the Bilingual Services Translation Act of 1977 to repeal redundant provisions.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "Language Access Act of 2004".

Sec. 2. Definitions.

For purposes of this act, the term:

(1) "Access or participate" means to be informed of, participate in, and benefit from public services, programs, and activities offered by a covered entity at a level equal to English proficient individuals.

(2) "Covered entity" means any District government agency, department, or program that furnishes information or renders services, programs, or activities directly to the public or contracts with other entities, either directly or indirectly, to conduct programs, services, or activities. The term "covered entity" shall not include the Advisory Neighborhood Commissions.

(3)(A) "Covered entity with major public contact" means a covered entity whose primary responsibility consists of meeting, contracting, and dealing with the public.

(B) Covered entities with major public contact are:

(i) Alcoholic Beverage Regulation Administration;
(ii) Department of Health;
(iii) Department of Mental Health;
(iv) Department of Human Services;
(v) Department of Employment Services;
(vi) Fire and Emergency Medical Services;
(vii) District of Columbia Housing Authority;
(viii) District of Columbia general ambulatory and emergency care centers;
(ix) Emergency Management Agency;
(x) Metropolitan Police Department;
(xi) District of Columbia Public Schools;
(xii) Department of Motor Vehicles;
(xiii) Department of Housing and Community Development;
(xiv) Department of Public Works;
(xv) Department of Corrections;
(xvi) Office on Aging;
(xvii) District of Columbia Public Library;
(xviii) Department of Parks and Recreation ;
(xix) Department of Consumer and Regulatory Affairs ;
(xx) Child and Family Services Agency;
(xxi) Office of Human Rights;
(xxii) Office of Personnel;
(xxiii) Office of Planning;
(xxiv) Office of Contracting and Procurement;
(xxv) Office of Tax and Revenue; and
(xxvi) Office of the People's Counsel.

(C) Other covered entities with major public contact may be designated by the Language Access Director through the Mayor, by regulation, after consultation with the D. C. Language Access Coalition in accordance with section 6(b)(6).

(4) "Language Access Director" means the official in the Office of Human Rights who, pursuant to section 6, coordinates and supervises the activities of District agencies, departments, and programs undertaken to comply with the provisions of this act.

(5) "Limited or no-English proficiency" means the inability to adequately understand or to express oneself in the spoken or written English language.

(6) "Oral language services" means the provision of oral information necessary

to enable limited or no-English proficiency residents to access or participate in programs or services offered by a covered entity. The term "oral language services" shall include placement of bilingual staff in public contact positions; the provision of experienced and trained staff interpreters; contracting with telephone interpreter programs; contracting with private interpreter services; and using interpreters made available through community service organizations that are publicly funded for that purpose.

(7) "Vital documents" means applications, notices, complaint forms, legal contracts, and outreach materials published by a covered entity in a tangible format that inform individuals about their rights or eligibility requirements for benefits and participation. The term "vital documents" shall include tax-related educational and outreach materials produced by the Office of Tax and Revenue, but shall not include tax forms and instructions.

Sec. 3. Oral language services provided by covered entities.

(a) A covered entity shall provide oral language services to a person with limited or no-English proficiency who seeks to access or participate in the services, programs, or activities offered by the covered entity.

(b) A covered entity shall, at least annually, determine the type of oral language services needed based upon:

(1) The number or proportion of limited or no-English proficient persons of the population served or encountered, or likely to be served or encountered by the covered entity, in the District of Columbia;

(2) The frequency with which limited or no-English proficient individuals come into contact with the covered entity;

(3) The importance of the service provided by the covered entity; and

(4) The resources available to the covered entity.

(c)(1) In making the determination under subsection (b) of this section of the type of oral language services needed, the covered entity shall consult the following sources of data to determine the languages spoken and the number or proportion of limited or no-English proficient persons of the population that are served or encountered, or likely to be served or encountered, by the covered entity in the District of Columbia:

(A) The United States Census Bureau's most current report entitled "Language Use and English Ability, Linguistic Isolation" (or any other successor report);

(B) Any other language-related information;

(C) Census data on language ability indicating that individuals speak English "less than very well";

(D) Local census data relating to language use and English language ability;

(E) Other governmental data, including intake data collected by covered entities; data collected by the District of Columbia Public Schools; and data collected by and

made available by District government offices that conduct outreach to communities with limited-English proficient populations and that serve as a liaison between the District government and limited-English proficient populations, such as the Office of Latino Affairs and the Office of Asian and Pacific Islander Affairs; and

(F) Data collected and made available by the D.C. Language Access Coalition.

(2) A covered entity shall annually collect data about the languages spoken and the number or proportion of limited or no-English proficient persons speaking a given language in the population that is served or encountered, or likely to be served or encountered, by the covered entity. A covered entity's databases and tracking applications shall contain fields that will capture this information during the fiscal year that this act takes effect with respect to the covered entity pursuant to section 7. If it is demonstrated to the Office of Human Rights that this is not feasible due to budgetary constraints, a covered entity shall make all due efforts to comply with this paragraph by the beginning of the next fiscal year. All information collected under this section shall be provided to the Language Access Director and made available to the public, upon request, within a reasonable time.

(d) To the extent that a covered entity requires additional personnel to meet its requirement to provide oral language services based on the determination set forth in this section, the covered entity shall hire bilingual personnel into existing budgeted vacant public contact positions.

Sec. 4. Written language services by covered entity.

(a) A covered entity shall provide translations of vital documents into any non-English language spoken by a limited or no-English proficient population that constitutes 3% or 500 individuals, whichever is less, of the population served or encountered, or likely to be served or encountered, by the covered entity in the District of Columbia.

(b) If the provisions of this act are contractually imposed on a non-covered entity, subsection (a) of this section shall apply.

Sec. 5. Additional obligations of covered entities with major public contact.

(a)(1) A covered entity with major public contact shall establish a language access plan, by regulation.

(2) Each language access plan shall be established in consultation with the Language Access Director, the D.C. Language Access Coalition, the entity's language access coordinator, and agency directors that conduct outreach to limited or no-English populations. Each language access plan shall be updated every 2 years and shall set forth, at minimum, the following:

(A) The types of oral language services that the entity will provide and how the determination was reached;

(B) The titles of translated documents that the entity will provide and how the determination was reached;

(C) The number of public contact positions in the entity and the number of bilingual employees in public contact positions;

(D) An evaluation and assessment of the adequacy of the services to be provided; and

(E) A description of the funding and budgetary sources upon which the covered entity intends to rely to implement its language access plan.

(3) In establishing and updating the language access plan, the entity shall consult with the sources of data set forth in section 3(c)(1).

(b) A covered entity with major public contact shall designate a language access coordinator who shall report directly to the director of the entity and shall:

(1) Establish and implement the entity's language access plan in consultation with the Language Access Director, the D.C. Language Access Coalition, and the agency directors of government offices that conduct outreach to communities with limited or no-English proficient populations; and

(2) Conduct periodic public meetings with appropriate advance notice to the public.

(c) A covered entity with major public contact shall develop a plan to conduct outreach to communities with limited or no-English proficient populations about their language access plans and about the benefits and services to be offered under this act.

Sec. 6. Language access oversight; duties of Language Access Director.

(a) The Office of Human Rights shall provide oversight, central coordination, and technical assistance to covered entities in their implementation of the provisions of this act and ensure that the provision of services by covered entities meets acceptable standards of translation or interpretation.

(b) There shall be within the Office of Human Rights a Language Access Director to coordinate activities under this act. The Language Access Director shall:

(1) Review and monitor each covered entity's language access plan for compliance with this act and Title VI of the Civil Rights Act of 1964, approved July 2, 1964 (78 Stat. 252; 42 U.S.C. §§ 2000d through 2000d-7);

(2) Track, monitor, and investigate public complaints regarding language access violations at covered entities, and where necessary, issue written findings of noncompliance to the covered entities regarding failures to provide language access; provided, that this responsibility shall not supersede or preclude the existing individual complaint process and mechanism under the jurisdiction of the Office of Human Rights;

(3) Review and monitor the language access coordinators with respect to their performance of responsibilities under this act;

(4) Consult with language access coordinators, the D.C. Language Access Coalition, and the heads of government offices that conduct outreach to communities with limited or no-English proficient populations;

(5) Serve as the language access coordinator for the Office of Human Rights; and

(6) Through the Mayor, by regulation, after consultation with the D.C. Language Access Coalition, designate additional covered entities with major public contact.

Sec. 7. Phased implementation.

(a) This act shall apply on its effective date to:

(1) Department of Health;
(2) Department of Human Services;
(3) Department of Employment Services;
(4) Metropolitan Police Department;
(5) District of Columbia Public School System;
(6) Office of Planning;
(7) Fire and Emergency Medical Services; and
(8) Office of Human Rights.

(b) This act shall apply as of October 1, 2004 to:

(1) Department of Housing and Community Development;
(2) Department of Mental Health;
(3) Department of Motor Vehicles;
(4) Child and Family Services Agency;
(5) Alcoholic Beverage Regulation Administration; and
(6) Department of Consumer and Regulatory Affairs.

(c) This act shall apply as of October 1, 2005, to:

(1) Department of Parks and Recreation;
(2) Office on Aging;
(3) District of Columbia Public Library;
(4) Office of Personnel;
(5) Office of Contracting and Procurement;
(6) Department of Corrections;
(7) Department of Public Works; and
(8) Office of Tax and Revenue.

(d) This act shall apply as of October 1, 2006 to all covered entities.

Sec. 8. Conforming amendments.

(a) Section 304 of the District of Columbia Latino Community Development Act, effective September 29,1976 (D.C. Law 1-86; D.C. Official Code § 2-1314), is repealed.

(b) The Bilingual Translation Services Act of 1977, effective October 26, 1977 (D.C. Law 2-31; D.C. Official Code § 2-1342 *et seq.*), is repealed.

Sec. 9. Inclusion in the budget and financial plan.

This act shall take effect subject to the inclusion of its fiscal effect in an approved budget and financial plan. This act is subject to appropriations.

Sec. 10. Fiscal impact statement.

The Council adopts the fiscal impact statement in the committee report as the fiscal impact statement required by section 602(c)(3) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-206.02(c)(3)).

Sec. 11. Effective date.

This act shall take effect following approval by the Mayor (or in the event of veto by the Mayor, action by the Council to override the veto), a 30-day period of Congressional review as provided in section 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 831; D.C. Official Code § 1-206.02(c)(1)), and publication in the District of Columbia Register.

_____

Chairman
Council of the District of Columbia

_____

Mayor
District of Columbia

PAST PERFORMANCE EVALUATION FORM

(Check appropriate box)

Performance Elements	Excellent	Good	Acceptable	Poor	Unacceptable
Quality of Services/ Work					
Timeliness of Performance					
Cost Control					
Business Relations					
Customer Satisfaction					

1. Name & Title of Evaluator:_____

2. Signature of Evaluator:_____

3. Name of Organization: _____

4. Telephone Number of Evaluator:_____

5. State type of service received: _____

6. State Contract Number, Amount and period of Performance _____

   _____

7. Remarks on Excellent Performance: Provide data supporting this observation. Continue on separate sheet if needed)

8. Remarks on unacceptable performance: Provide data supporting this observation. (Continue on separate sheet if needed)

RATING GUIDELINES

Summarize Contractor performance in each of the rating areas. Assign each area a rating of 0 (Unacceptable), 1 (Poor), 2 (Acceptable), 3 (Good), 4(Excellent), or ++ (Plus). Use the following instructions a guidance in making these evaluations.

	Quality Product/Service	**Cost Control**	**Timeless of Performance**	**Business Relations**
	-Compliance with contract requirements -Accuracy of reports -Appropriateness of personnel -Technical excellence	-Within budget (over/ under target costs) -Current, accurate, and complete billings -Relationship of negated costs to actual -Cost efficiencies -Change order issue	-Meet Interim milestones -Reliable -Responsive to technical directions -Completed on time, including wrap-up and -contract administration -No liquidated damages assessed	-Effective management -Businesslike correspondence -Responsive to contract requirements -Prompt notification of contract problems -Reasonable/cooperative -Flexible -Pro-active -effective contractor recommended solutions -Effective snail/small disadvantaged business Subcontracting program
0. Zero	Nonconformances are comprises the achievement of contract requirements, despite use of Agency resources	Cost issues are comprising performance of contract requirements.	Delays are comprising the achievement of contract requirements, Despite use of Agency resources.	Response to inquiries, technic al/ service/administrative issues is not effective and responsive.
1, Unacceptable	Nonconformances require major Agency resources to ensure achievement of contract requirements.	Cost issues require major Agency resources to ensure achievement of contract requirements.	Delays require major Agency resources to ensure achievement of contract requirements.	response to inquiries, technical/ service/administrative issues is marginally effective and responsive.
2. Poor	Nonconformances require minor Agency resources to ensure achievement of contract requirements.	Costs issues require minor Agency resources to ensure achievement of contract requirements.	Delays require minor Agency resources to ensure achievement of contract requirements.	Responses to inquiries, technical/ service/administrative issues is somewhat effective and responsive.
3. Acceptable	Nonconformances do not impact achievement of contract requirements.	Cost issues do not impact achievement of contract requirements.	Delays do not impact achievement of contract requirements.	Responses to inquires, technical/ service/administrative issues is usually effective and responsive.
4. Good	There are no quality problems.	There are no cost issues.	There are not delays.	Responses to inquiries, technical/ service/administrative issues is effective and responsive,
5. Excellent	The contractor has demonstrated an exceptional performance level in some or all of the above categories.			

Office of Contracting and Procurement
Government of the District of Columbia

COST / PRICE DISCLOSURE CERTIFICATION

RFP Number: **DCHC-2007-R-5050** Closing Date**:** **May 8, 2007**

Caption: **Managed Care Organizations Healthcare Services DC Healthy Families and DC Healthcare Safety Net Programs** Total Proposed Amount: _____

The undersigned _____
_____
(please print name and title of offeror' s authorized signatory) hereby certifies that, to the best of my knowledge, the cost and pricing data (i.e. at the time of price agreement this certification represents that all material facts of which prudent buyers and sellers would reasonably expect to affect price negotiations in any significant manner) submitted was accurate, complete, and current as of _____ (date of RFP closing or conclusion of negotiations as appropriate) . The undersigned further agrees that it is under a continuing duty to update cost or pricing data through the date that negotiations, if any, with the District are completed. The undersigned further agrees that the price, including profit or fee, will be adjusted to exclude any significant price increases occurring because the cost or pricing data was inaccurate, incomplete or not current. (See D.C. Procurement Regulations, 27 DCMR, Chapter 6, Section 699, Chapter 16, Section 1624; and Section 32 of the Standard Contract Provisions for Use with District of Columbia Government Supply and Services Contracts, December 1984, as amended).

Signed: _____ Date:_____

Title: _____

Company: _____

Address: _____

_____

DUNS #:_____

Phone: _____

Fax: _____

COST/PRICE DATA REQUIREMENTS

1. GENERAL INFORMATION:

1.1 Offerors submitting cost/price proposals, in response to a District Request For Proposal (RFP), sole source procurement, change order, or contract modification exceeding $500,000 in total value, must include a complete cost and pricing data breakdown (i.e., data that is verifiable and factual) for all costs identified in the proposal, and relevant to the performance of the contract. The requirement for submission of cost or pricing data is met when all accurate cost or pricing data reasonably available to the Offeror has been submitted, either actually, or by specific identification, to the District. If not available at the time of submission, as later information comes into the Offeror's possession, it should be promptly submitted to the District in a manner that clearly demonstrates its relationship to, and effect on, the Offeror's cost/price proposal. This requirement continues up to the date of final agreement on price and/or other issues, as agreed upon between the parties.

1.2 There is a clear distinction between submitting cost or pricing data and merely making available books, records and other documents without identification or context. By submitting a cost/price proposal, the Offferor, if selected for negotiation, grants the Contracting Officer, or an authorized representative, the right to examine, at any time before award, those books, records, documents, and other types of factual information, regardless of form or whether such supporting information is specifically referenced or included in the proposal as a basis for pricing, that will permit an adequate evaluation of the proposed cost/price.

1.3 The cost/price proposal will represent the offeror's understanding of the RFP's requirements and the offeror's ability to organize and perform those requirements effectively and efficiently. The evaluation of the Offeror's cost/price proposal will be based on an analysis of the realism and completeness of the cost data, the conformity of the cost to the offeror's technical data and the proposed allocation of labor-hours and skill sets. Pertinent cost information, including but not limited to Defense Contract Auditing Agency (DCAA) and/or the Department of Labor (DOL) recommended rates for direct labor, overhead, general and administrative expense (G&A), etc., as necessary and appropriate, must be used to arrive at the most probable cost to be incurred by the Offeror. If the District considers the proposed costs to be unrealistic, the Offeror should adjust its proposed costs accordingly. Any inconsistency, whether real or apparent, between promised performance and cost or price should be explained in the cost/price proposal. The burden of proof for cost credibility rests with the Offeror.

1.4 The Offeror must submit its cost/price proposal in hard copy as well as on a diskette, which is in a format (i.e. MS Office, Lotus 1-2-3, etc.) specified and/or provided by the Agency Contracting Officer in the solicitation package. All cost/price proposals should provide a cost summary by all cost elements, cross-referenced to supporting documentation. See Table No. (1.4).

1.5 The following information shall be included in this section, for the prime contractor and each proposed subcontractor:

(a) A properly completed "Cost/Price Disclosure Certification.'

(a) Identification of any estimates, along with the rationale and methodology used to develop them, including judgmental factors used in projecting future costs, based on known data, and the timing, nature and extent of any material contingencies.

(c) Disclosure of any other activities or likely events which could materially impact specific costs (i.e., existing large material and supply inventories, management/ownership changes, new technologies, collective bargaining agreements, etc.)

(d) Disclosure of any and all awarded and pending contracts with the District of Columbia, including contract number(s), amount, type (fixed price, cost reimbursement, etc.), agency, and a brief description of services.

(e) Source of approval and the latest date of approval of the offeror' s Accounting system.

Table (1.4)

Example Cost Summary Format

Cost Item	Task 1			Task 2			Task 3			Task 4, etc.			Base Year Total
Direct Labor Categories • Employee A • Employee B • Employee C Total Labor Hours	R	H	D	R	H	D	R	H	D	R	H	D	
Total Labor Dollars													
Fringe Benefit													
Labor Overhead *													
Total Direct Labor													
Other Direct Costs • Equip. & Supplies • Materials • Travel • Other													
Subcontractors • Sub A • Sub B													
ODC Overhead *													
Total ODC & Subcontractors													
G&A													
Fee/Profit													
Total Price													

H = Hours R = Rate D = Dollars (Rate X Hours = Dollars)

Note:Provide cost information similar to the above format for each option/out-year

** Note: Small, field-based trade providers typically have a labor or combined overhead cost components. Larger, more diversified providers may have separate labor, and/or ODC or combined overhead component.*

2. SUPPORTING COST DATA:

2.1 The Offeror shall provide, for each cost element, a narrative description, in sufficient detail, to demonstrate price reasonableness, credibility and reliability. The Offeror shall provide its assumptions and methodologies used to estimate each cost element (significant item and quantity estimates, labor hour expenditure patterns and mix, etc.). The following information shall be included in this section:

2.1.1. The Offeror's total estimated costs plus its fee (if applicable) for providing all of the requirements of the RFP, as proposed in their technical proposal. Offerors should support their best estimates of all costs (direct, indirect, profit, etc.) to be incurred in the performance of the contract.

2.1.2. When proposing multiyear/option year pricing, the estimated proposed costs shall include a breakdown of all cost elements for the base year as well as each option/out-year. Labor, other direct costs, indirect costs and profit shall each be clearly identifiable. If different from the Defense Contract Auditing Agency (DCAA) or Department Of Labor (DOL) recommended rates, the Offeror shall provide a thorough explanation for the variation(s) of rates.

2.1.3. The Cost Summary Format (Table1.4) provides a format for the Offeror to submit to the District a pricing proposal of estimated cost by line item, along with supporting documentation that is adequately cross-referenced and suitable for cost realism analysis. A cost-element breakdown shall be attached for each proposed line item and must reflect any other specific requirements established by the Contracting Officer. When more than one contract line item is proposed, a summary of the total amount covering all line items must be furnished for each cost element.

2.1.4. If the Offeror has an agreement with a federal, state, or municipal government agency on the use of a Forward Pricing Rates Agreement (FPRA) or other rate agreement for labor, fringe benefits, overhead and/or general and administrative expense, the Offeror must identify the agreement, provide a copy and describe its nature, terms and duration.

3. SPECIFIC COST ELEMENTS:

A well-supported cost/price proposal reduces the effort needed for review and facilitates informed negotiations. The following are the minimum criteria that constitute an acceptable cost/price proposal:

3.1 **Direct labor:** A task-phased annual breakdown of labor rates and labor hours by category or skill level, including the basis for the rates and hours estimated (i.e., payroll registers, wage determinations, collective bargaining agreements, historical experience, engineering estimates, etc.).

3.1.1 The Offeror shall use the following Table No. (3.1.1) to exhibit its total labor hours by prime contractor and subcontractor(s). A separate table should be completed for each year (base and out-years).

Table (3.1.1)

Annual Labor Summary

Item	Task 1	Task 2	Task 3	Task 4	Base Year Total
Labor Category, Prime • Employee A • Employee B • Employee C Labor Category, Sub. • Employee D • Employee E • Employee F Labor Category, Consultant • Employee G • Employee H					
Total Labor Hours by Task					

Note: Do not include wage rates in this table

3.1.2 A standard of 40 hours/week, 1,920 hours/year is recommended. If another standard is used, it should be precisely defined. Any deviation from the above labor-hour projection without substantiation may form the basis to reject the response to the RFP. The proposed labor-hours shall include prime contractor, subcontractor and consultant hours.

3.1.3 The Offeror shall also submit Table No. (3.1.4.b), depicting the labor mix percentages as proposed for the base year as well as the out-years and should match the personnel experience requirements specified in the RFP, Section **(to be referenced by the Contract Specialist),** under Personnel Experience. All of the RFP Key positions must be included within the Senior Staff categories. To provide a better understanding of this format, Table No. (3.1.4.a) is provided as an example.

3.1.4 The Offeror shall describe how the hourly direct labor rate was derived and indicate whether these rates are subject to any collective bargaining agreement(s), the Service Contract Act (SCA), Davis-Bacon, or any other special agreement which controls the labor rate indicated. When proposing price escalation for option/out-years, the Offerors must follow instructions provided under Economic Price Adjustments, Section H, of this RFP.

Table (3.1.4.a)

Summary of Proposed Annual labor Mix Category (with examples)

NAME (Note1)	LABOR MIX (Note 2)	OFFEROR'S LABOR CATEGORY (Note 3)	PERCENT OF TIME ON CONTRACT (Note 4)	PLANNED SOW ASSIGNMENT (Note 5)	STATUS (Note 6)
Able, Jackson	Sr. Staff Level 1	Program Director	PT/10%	N/A	PCE/E
Black, William E.	Sr. Staff Level 1	Psychiatrist	PT/20%	C.3	PCE/E
White, Pamela A.	Sr. Staff Level 2	Clinic Manager	PT/50%	C.4.1	PCE/P
Green, Robert T	Sr. Staff Level 3	Counseling Supvs.	PT/50%	C.4.2	PCE/P
Ross, Allen	Jr. Staff Level 1	Counselor	FT/100%	C.4.3	PCE/E

Note 1: Last name, first name, middle initial, grouped by task as specified in SOW. Attach resume for each name on list. The names on this list and the resumes are to be in the same order.

Note 2: Staff levels in each Labor Mix should be classified by the level of expertise and years of experience.

Note 3: Offerors internal labor category.

Note 4: State whether the individual is employed full time (FT) or part time (PT) and the planned percentage of the named person's production time that is to be applied as a direct charge to the contract.

Note 5: Identify by SOW paragraph(s) and task number, the major tasks to which the individual is expected to be assigned.

Note 6: Enter PCE if individual is to be a prime contractor employee; enter SCE if the individual is to be a subcontractor employee; enter CON if individual is to be a consultant. Enter E if employee as of the date of this proposal; enter P if the individual is a pending employee as of date of the proposal. Signed Commitment Agreements are required for all individuals with P status. A copy of each agreement is to be inserted behind the resume section in the technical proposal.

Table (3.1.4.b)

Summary of Proposed Annual labor Mix Category

NAME (Note1)	LABOR MIX (Note 2)	OFFEROR' S LABOR CATEGORY (Note 3)	PERCENT OF TIME ON CONTRACT (Note 4)	PLANNED SOW ASSIGNMENT (Note 5)	STATUS (Note 6)
Labor Category, Prime • Employee A • Employee B • Employee C • Employee D Labor Category, Sub. • Employee E • Employee F • Employee G Labor Category, Consultant • Employee H Employee I					

Last name, first name, middle initial, grouped by task as specified in SOW. Attach resume for each name on list. The names on this list and the resumes are to be in the same order.

Note 2: Staff levels in each Labor Mix should be classified by the level of expertise and years of experience.

Note 3: Offerors internal labor category.

Note 4: State whether the individual is employed full time (FT) or part time (PT) and the planned percentage of the named person's production time that is to be applied as a direct charge to the contract.

Note 5: Identify by SOW paragraph(s) and task number, the major tasks to which the individual is expected to be assigned.

Note 6: Enter PCE if individual is to be a prime contractor employee; enter SCE if the individual is to be a subcontractor employee; enter CON if individual is to be a consultant. Enter E if employee as of the date of this proposal; enter P if the individual is a pending employee as of date of the proposal. Signed Commitment Agreements are required for all individuals with P status. A copy of each agreement is to be inserted behind the resume section in the technical proposal.

3.2 **Indirect Costs:** The Offeror shall indicate it's proposed Fringe, Overhead and General & Administrative rates for each applicable fiscal or calendar year (as appropriate). The Offeror shall indicate if these rates are subject to a Forward Pricing Rate Agreement. If the proposed Indirect Rates differ from the Forward Pricing Rate Agreement, the Offeror shall provide an explanation. The Offeror shall provide its actual indirect rates for overhead, G&A and fringe benefits for at least the past three (3) years and shall explain the basis for any significant rate difference between the prior three year period and the rates proposed now.

3.3 **Other Direct Costs:** Other Direct Costs consists of materials, travel, reproduction, postage, telephone, supplies for the prime and all subcontracted effort. This includes all other direct costs associated with performance of the contract. Travel costs shall be in accordance with GSA Joint Travel Regulations for airfare, hotel, and per diem allowances. All other direct costs should be specifically identified and explained. If an allocated portion of a Direct cost is also included in an Offeror's indirect rate (such as General and Administrative), the Offeror should state so and list the types of expenses included in the indirect rate.

3.3.1 The Offeror should identify types, quantities, and costs of all materials and supplies proposed including a non-loaded priced listing of individual materials or supplies ordered, or a consolidated and priced bill of materials for the entire proposal. A thoroughly documented bill of materials includes part numbers, description, unit costs, quantity required, extended cost (including delivery charges) and basis for the proposed cost (price quotation, prior buy, signed purchase orders, etc.) plus any other non-recurring costs. Deliverable materials are items delivered as a part of the work product. Examples of this are copies and binders delivered to the Government as a report or software ordered for and installed on a computer in a District Government office.

3.3.2 The Offeror shall use the following Table (3.3.2) to exhibit its total other direct costs (ODC) by prime and subcontractor(s). A separate table should be completed for each year (base and out-years).

Table (3.3.2)

Other Direct Costs (ODC) Summary

Item	Task 1	Task 2	Task 3	Task 4	Base Year Total
Supplies and Materials Office Equipment Travel • Airfare • Hotel • Meals & Incidentals • Ground Transportation Telecommunications Occupancy • Rent • Utilities • Building Maintenance Transportation Client Care Cost • Food • Medical • Clothing • Personal Hygiene Other					
Total ODC by Task					

Note: *State each individual cost element being proposed. Describe in the narrative section of the cost proposal, how each cost element is derived and why it is being proposed. (Not all cost elements in the table above will apply to each solicitation. The above table should be tailored to the requirements of the RFP.)*

3.4 **Subcontracting Costs:** Each subcontract must be addressed separately. For any subcontract exceeding $25,000 the cost/price proposal must show the names, quantities, prices, deliverables, basis for selection, and degree of competition used in the selection process. The subcontractor's cost or pricing data should be included along with the prime Offeror's proposal. If available, the Offeror should also include the results of its review and evaluation of the subcontract proposals. The Offeror shall provide copies of any cost or price analyses of the subcontractor costs proposed.

3.5 **Start-up Costs:** As appropriate, the Offeror shall identify all start up costs associated with this effort.

3.6 **Other Historical Data:** All offerors with current or past experience (within three to five years) for similar requirements, as described herein, must submit, as a part of their cost data, the following:

(a) Contract Number.

(b) Government agency (federal, state, District, municipal) the contract was awarded by.

(c) Name and phone number of the Contracting Officer.

(d) Name and phone number of the Contract Administrator.

(e) Name and phone number of the Contracting Officer' s Representative (if applicable) and the Contract Administrator.

(f) Period of Performance of the Contract.

(g) Total amount of contract(s)

In addition to the above data, the following table (No. 3.6) will be completed and submitted with the cost data:

Table (3.6)

Format for Historical Data

	Proposed Contract			**Delivered Contract ***		
	Number Of Hours**	Contract Value	Average Hr Rate	Number Of Hours**	Contract Value	Average Hr Rate
Direct Labor						
Loaded Labor***						

* Should include any increased scope officially added to contract.
** If provided different number of hours, the difference should be explained.
*** Loaded labor should include all loading and profit. If significant material (i.e., greater than 5%) is included in the contract, data shall be presented both with and without material cost.

In addition, any other data the offeror believes is necessary should be provided in this section.

Note: For data submitted in the above table for "delivered Contract", the Offeror shall indicate the date as of which, the submitted data is current.

[TABLE OF CONTENTS] [SUMMARY]

PUBLIC LAW 104-191

AUG. 21, 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104-191
104th Congress

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**--This Act may be cited as the "Health Insurance Portability and Accountability Act of 1996".

(b) **TABLE OF CONTENTS.**--The table of contents of this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I--HEALTH CARE ACCESS, PORTABILITY, AND RENEWABILITY

...

TITLE II--PREVENTING HEALTH CARE FRAUD AND ABUSE; ADMINISTRATIVE SIMPLIFICATION; MEDICAL LIABILITY REFORM

...

Subtitle F--Administrative Simplification

- Sec. 261. Purpose.
- Sec. 262. Administrative simplification.

"Part C--Administrative Simplification

- "Sec. 1171. Definitions.
- "Sec. 1172. General requirements for adoption of standards.
- "Sec. 1173. Standards for information transactions and data elements.
- "Sec. 1174. Timetables for adoption of standards.
- "Sec. 1175. Requirements.
- "Sec. 1176. General penalty for failure to comply with requirements and standards.
- "Sec. 1177. Wrongful disclosure of individually identifiable health information.
- "Sec. 1178. Effect on State law.
- "Sec. 1179. Processing payment transactions.".

Sec. 263. Changes in membership and duties of National Committee on Vital and Health Statistics.

Sec. 264. Recommendations with respect to privacy of certain health information.

...

Subtitle F--Administrative Simplification

SEC. 261. PURPOSE.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.

SEC. 262. ADMINISTRATIVE SIMPLIFICATION.

(a) IN GENERAL.--Title XI (42 U.S.C. 1301 et seq.) is amended by adding at the end the following:

"PART C--ADMINISTRATIVE SIMPLIFICATION

"DEFINITIONS

"**SEC. 1171**. For purposes of this part:

"(1) CODE SET.--The term 'code set' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

"(2) HEALTH CARE CLEARINGHOUSE.--The term 'health care clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

"(3) HEALTH CARE PROVIDER.--The term 'health care provider' includes a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)), and any other person furnishing health care services or supplies.

"(4) HEALTH INFORMATION.--The term 'health information' means any information, whether oral or recorded in any form or medium, that--

"(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

"(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

"(5) HEALTH PLAN.--The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act). Such term includes the following, and any combination thereof:

"(A) A group health plan (as defined in section 2791(a) of the Public Health Service Act), but only if the plan--

"(i) has 50 or more participants (as defined in section 3(7) of the Employee Retirement Income Security Act of 1974); or

"(ii) is administered by an entity other than the employer who established and maintains the plan.

"(B) A health insurance issuer (as defined in section 2791(b) of the Public Health Service Act).

"(C) A health maintenance organization (as defined in section 2791(b) of the Public Health Service Act).

"(D) Part A or part B of the Medicare program under title XVIII.

"(E) The medicaid program under title XIX.

"(F) A Medicare supplemental policy (as defined in section 1882(g)(1)).

"(G) A long-term care policy, including a nursing home fixed indemnity policy (unless the Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).

"(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.

"(I) The health care program for active military personnel under title 10, United States Code.

"(J) The veterans health care program under chapter 17 of title 38, United States Code.

"(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of title 10, United States Code.

"(L) The Indian health service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.).

"(M) The Federal Employees Health Benefit Plan under chapter 89 of title 5, United States Code.

"(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.--The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that--

"(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

"(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--

"(i) identifies the individual; or

"(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

"(7) STANDARD.--The term 'standard', when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174.

"(8) STANDARD SETTING ORGANIZATION.--The term 'standard setting organization' means a standard setting organization accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation of this part.

"GENERAL REQUIREMENTS FOR ADOPTION OF STANDARDS

"**SEC. 1172.** (a) APPLICABILITY.--Any standard adopted under this part shall apply, in whole or in part, to the following persons:

"(1) A health plan.

"(2) A health care clearinghouse.

"(3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).

"(b) REDUCTION OF COSTS.--Any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.

"(c) ROLE OF STANDARD SETTING ORGANIZATIONS.--

"(1) IN GENERAL.--Except as provided in paragraph (2), any standard adopted under this part shall be a standard that has been developed, adopted, or modified by a standard setting organization.

"(2) SPECIAL RULES.--

"(A) DIFFERENT STANDARDS.--The Secretary may adopt a standard that is different from any standard developed, adopted, or modified by a standard setting organization, if--

"(i) the different standard will substantially reduce administrative costs to health care providers and health plans compared to the alternatives; and

"(ii) the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5, United States Code.

"(B) NO STANDARD BY STANDARD SETTING ORGANIZATION.--If no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt under this part--

"(i) paragraph (1) shall not apply; and

"(ii) subsection (f) shall apply.

(3) CONSULTATION REQUIREMENT.--

"(A) IN GENERAL.--A standard may not be adopted under this part unless--

"(i) in the case of a standard that has been developed, adopted, or modified by a standard setting organization, the organization consulted with each of the organizations described in subparagraph (B) in the course of such development, adoption, or modification; and

"(ii) in the case of any other standard, the Secretary, in complying with the requirements of subsection (f), consulted with each of the organizations described in subparagraph (B) before adopting the standard.

"(B) ORGANIZATIONS DESCRIBED.--The organizations referred to in subparagraph (A) are the following:

"(i) The National Uniform Billing Committee.

"(ii) The National Uniform Claim Committee.

"(iii) The Workgroup for Electronic Data Interchange.

"(iv) The American Dental Association.

"(d) IMPLEMENTATION SPECIFICATIONS.--The Secretary shall establish

specifications for implementing each of the standards adopted under this

part.

"(e) PROTECTION OF TRADE SECRETS.--Except as otherwise required by law, a standard adopted under this part shall not require disclosure of trade secrets or confidential commercial information by a person required to comply with this part.

"(f) ASSISTANCE TO THE SECRETARY.--In complying with the requirements of this part, the Secretary shall rely on the recommendations of the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)), and shall consult with appropriate Federal and State agencies and private organizations. The Secretary shall publish in the Federal Register any recommendation of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.

(g) APPLICATION TO MODIFICATIONS OF STANDARDS.--This section shall apply to a modification to a standard (including an addition to a standard) adopted under section

1174(b) in the same manner as it applies to an initial standard adopted under section 1174(a).

"STANDARDS FOR INFORMATION TRANSACTIONS AND DATA ELEMENTS

"**SEC. 1173.** (a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.--

"(1) IN GENERAL.--The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for--

"(A) the financial and administrative transactions described in paragraph (2); and

"(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

"(2) TRANSACTIONS.--The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

"(A) Health claims or equivalent encounter information.

"(B) Health claims attachments.

"(C) Enrollment and disenrollment in a health plan.

"(D) Eligibility for a health plan.

"(E) Health care payment and remittance advice.

"(F) Health plan premium payments.

"(G) First report of injury.

"(H) Health claim status.

"(I) Referral certification and authorization.

"(3) ACCOMMODATION OF SPECIFIC PROVIDERS.--The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

(b) UNIQUE HEALTH IDENTIFIERS.--

"(1) IN GENERAL.--The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for

use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

"(2) USE OF IDENTIFIERS.--The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

(c) CODE SETS.--

"(1) IN GENERAL.--The Secretary shall adopt standards that--

"(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) from among the code sets that have been developed by private and public entities; or

"(B) establish code sets for such data elements if no code sets for the data elements have been developed.

"(2) DISTRIBUTION.--The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

(d) SECURITY STANDARDS FOR HEALTH INFORMATION.--

"(1) SECURITY STANDARDS.--The Secretary shall adopt security standards that--

"(A) take into account--

"(i) the technical capabilities of record systems used to maintain health information;

"(ii) the costs of security measures;

"(iii) the need for training persons who have access to health information;

"(iv) the value of audit trails in computerized record systems; and

"(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

"(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

"(2) SAFEGUARDS.--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--

"(A) to ensure the integrity and confidentiality of the information;

"(B) to protect against any reasonably anticipated--

"(i) threats or hazards to the security or integrity of the information; and

"(ii) unauthorized uses or disclosures of the information; and

"(C) otherwise to ensure compliance with this part by the officers and employees of such person.

(e) ELECTRONIC SIGNATURE.--

"(1) STANDARDS.--The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).

"(2) EFFECT OF COMPLIANCE.--Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

(f) TRANSFER OF INFORMATION AMONG HEALTH PLANS.--The Secretary shall adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan.

"TIMETABLES FOR ADOPTION OF STANDARDS

"**SEC. 1174.** (a) INITIAL STANDARDS.--The Secretary shall carry out section 1173 not later than 18 months after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, except that standards relating to claims attachments shall be adopted not later than 30 months after such date.

"(b) ADDITIONS AND MODIFICATIONS TO STANDARDS.--

"(1) IN GENERAL.--Except as provided in paragraph (2), the Secretary shall review the standards adopted under section 1173, and shall adopt modifications to the standards (including additions to the standards), as determined appropriate, but not more frequently than once every 12 months. Any addition or modification to a standard shall be completed in a manner which minimizes the disruption and cost of compliance.

"(2) SPECIAL RULES.--

"(A) FIRST 12-MONTH PERIOD.--Except with respect to additions and modifications to code sets under subparagraph (B), the Secretary may not adopt any modification to a standard adopted under this part during the 12-month period beginning on the date the standard is initially adopted, unless the Secretary determines that the modification is necessary in order to permit compliance with the standard.

"(B) ADDITIONS AND MODIFICATIONS TO CODE SETS.--

"(i) IN GENERAL.--The Secretary shall ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets.

"(ii) Additional rules.--If a code set is modified under this subsection, the modified code set shall include instructions on how data elements of health information that were encoded prior to the modification may be converted or translated so as to preserve the informational value of the data elements that existed before the modification. Any modification to a code set under this subsection shall be implemented in a manner that minimizes the disruption and cost of complying with such modification.

"REQUIREMENTS

"**SEC. 1175.** (a) CONDUCT OF TRANSACTIONS BY PLANS.--

"(1) IN GENERAL.--If a person desires to conduct a transaction referred to in section 1173(a)(1) with a health plan as a standard transaction--

"(A) the health plan may not refuse to conduct such transaction as a standard transaction;

"(B) the insurance plan may not delay such transaction, or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the ground that the transaction is a standard transaction; and

"(C) the information transmitted and received in connection with the transaction shall be in the form of standard data elements of health information.

"(2) SATISFACTION OF REQUIREMENTS.--A health plan may satisfy the requirements under paragraph (1) by--

"(A) directly transmitting and receiving standard data elements of health information; or

"(B) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse, and receiving standard data elements through the health care clearinghouse.

"(3) TIMETABLE FOR COMPLIANCE.--Paragraph (1) shall not be construed to require a health plan to comply with any standard, implementation specification, or modification to a standard or specification adopted or established by the Secretary under sections 1172 through 1174 at any time prior to the date on which the plan is required to comply with the standard or specification under subsection (b).

"(b) COMPLIANCE WITH STANDARDS.--

"(1) INITIAL COMPLIANCE.--

"(A) IN GENERAL.--Not later than 24 months after the date on which an initial standard or implementation specification is adopted or established under sections 1172 and 1173, each person to whom the standard or implementation specification applies shall comply with the standard or specification.

"(B) SPECIAL RULE FOR SMALL HEALTH PLANS.--In the case of a small health plan, paragraph (1) shall be applied by substituting '36 months' for '24 months'. For purposes of this subsection, the Secretary shall determine the plans that qualify as small health plans.

"(2) COMPLIANCE WITH MODIFIED STANDARDS.--If the Secretary adopts a modification to a standard or implementation specification under this part, each person to whom the standard or implementation specification applies shall comply with the modified standard or implementation specification at such time as the Secretary determines appropriate, taking into account the time needed to comply due to the nature and extent of the modification. The time determined appropriate under the preceding sentence may not be earlier than the last day of the 180-day period beginning on the date such modification is adopted. The Secretary may extend the time for compliance for small health plans, if the Secretary determines that such extension is appropriate.

"(3) CONSTRUCTION.--Nothing in this subsection shall be construed to prohibit any person from complying with a standard or specification by--

"(A) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse; or

"(B) receiving standard data elements through a health care clearinghouse.

"GENERAL PENALTY FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS

"**SEC. 1176.** (a) GENERAL PENALTY.--

"(1) IN GENERAL.--Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each

such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.

"(2) PROCEDURES.--The provisions of section 1128A (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1128A.

"(b) LIMITATIONS.--

"(1) OFFENSES OTHERWISE PUNISHABLE.--A penalty may not be imposed under subsection (a) with respect to an act if the act constitutes an offense punishable under section 1177.

"(2) NONCOMPLIANCE NOT DISCOVERED.--A penalty may not be imposed under subsection (a) with respect to a provision of this part if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.

"(3) FAILURES DUE TO REASONABLE CAUSE.--

"(A) IN GENERAL.--Except as provided in subparagraph (B), a penalty may not be imposed under subsection (a) if--

"(i) the failure to comply was due to reasonable cause and not to willful neglect; and

"(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

"(B) EXTENSION OF PERIOD.--

"(i) NO PENALTY.--The period referred to in subparagraph (A)(ii) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure to comply.

"(ii) ASSISTANCE.--If the Secretary determines that a person failed to comply because the person was unable to comply, the Secretary may provide technical assistance to the person during the period described in subparagraph (A)(ii). Such assistance shall be provided in any manner determined appropriate by the Secretary.

"(4) REDUCTION.--In the case of a failure to comply which is due to reasonable cause and not to willful neglect, any penalty under subsection (a) that is not entirely waived under paragraph (3) may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

"WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

"**SEC. 1177.** (a) OFFENSE.--A person who knowingly and in violation of this part--

"(1) uses or causes to be used a unique health identifier;

"(2) obtains individually identifiable health information relating to an individual; or

"(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b).

"(b) PENALTIES.--A person described in subsection (a) shall--

"(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

"(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

"(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

"EFFECT ON STATE LAW

"**SEC. 1178.** (a) GENERAL EFFECT.--

"(1) GENERAL RULE.--Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

"(2) EXCEPTIONS.--A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall not supersede a contrary provision of State law, if the provision of State law--

"(A) is a provision the Secretary determines--

"(i) is necessary--

"(I) to prevent fraud and abuse;

"(II) to ensure appropriate State regulation of insurance and health plans;

"(III) for State reporting on health care delivery or costs; or

"(IV) for other purposes; or

"(ii) addresses controlled substances; or

"(B) subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.

"(b) PUBLIC HEALTH.--Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

"(c) STATE REGULATORY REPORTING.--Nothing in this part shall limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

"PROCESSING PAYMENT TRANSACTIONS BY FINANCIAL INSTITUTIONS

"**SEC. 1179.** To the extent that an entity is engaged in activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing,

transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

"(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.

"(2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph (1)--

"(A) for transferring receivables;

"(B) for auditing;

"(C) in connection with--

"(i) a customer dispute; or

"(ii) an inquiry from, or to, a customer;

"(D) in a communication to a customer of the entity regarding the customer's transactions, payment card, account, check, or electronic funds transfer;

"(E) for reporting to consumer reporting agencies; or

"(F) for complying with--

"(i) a civil or criminal subpoena; or

"(ii) a Federal or State law regulating the entity.".

(b) CONFORMING AMENDMENTS.--

(1) REQUIREMENT FOR MEDICARE PROVIDERS.--Section 1866(a)(1) (42 U.S.C. 1395cc(a)(1)) is amended--

(A) by striking ``and" at the end of subparagraph (P);

(B) by striking the period at the end of subparagraph (Q) and inserting "; and"; and

(C) by inserting immediately after subparagraph (Q) the following new subparagraph:

"(R) to contract only with a health care clearinghouse (as defined in section 1171) that meets each standard and implementation specification adopted or established under part C of title XI on or after the date on which the health care clearinghouse is required to comply with the standard or specification.".

(2) TITLE HEADING.--Title XI (42 U.S.C. 1301 et seq.) is amended by striking the title heading and inserting the following:

"TITLE XI--GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION".

SEC. 263. CHANGES IN MEMBERSHIP AND DUTIES OF NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS.

Section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k))

is amended--

(1) in paragraph (1), by striking "16" and inserting "18";

(2) by amending paragraph (2) to read as follows:

"(2) The members of the Committee shall be appointed from among persons who have distinguished themselves in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. Members of the Committee shall be appointed for terms of 4 years.";

(3) by redesignating paragraphs (3) through (5) as paragraphs (4) through (6), respectively, and inserting after paragraph (2) the following:

"(3) Of the members of the Committee--

"(A) 1 shall be appointed, not later than 60 days after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, by the Speaker of the House of Representatives after consultation with the Minority Leader of the House of Representatives;

"(B) 1 shall be appointed, not later than 60 days after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, by the President pro tempore of the Senate after consultation with the Minority Leader of the Senate; and

"(C) 16 shall be appointed by the Secretary.";

(4) by amending paragraph (5) (as so redesignated) to read as follows:

"(5) The Committee--

"(A) shall assist and advise the Secretary--

"(i) to delineate statistical problems bearing on health and health services which are of national or international interest;

"(ii) to stimulate studies of such problems by other organizations and agencies whenever possible or to make investigations of such problems through subcommittees;

"(iii) to determine, approve, and revise the terms, definitions, classifications, and guidelines for assessing health status and health services, their distribution and costs, for use (I) within the Department of Health and Human Services, (II) by all programs administered or funded by the Secretary, including the Federal-State-local cooperative health statistics system referred to in subsection (e), and (III) to the extent possible as determined by the head of the agency involved, by the Department of Veterans Affairs, the Department of Defense, and other Federal agencies concerned with health and health services;

"(iv) with respect to the design of and approval of health statistical and health information systems concerned with the collection, processing, and tabulation of health statistics within the Department of Health and Human Services, with respect to the Cooperative Health Statistics System established under subsection (e), and with respect to the standardized means for the collection of health information and statistics to be established by the Secretary under subsection (j)(1);

"(v) to review and comment on findings and proposals developed by other organizations and agencies and to make recommendations for their adoption or implementation by local, State, national, or international agencies;

"(vi) to cooperate with national committees of other countries and with the World Health Organization and other national agencies in the studies of problems of mutual interest;

"(vii) to issue an annual report on the state of the Nation's health, its health services, their costs and distributions, and to make proposals for improvement of the Nation's health statistics and health information systems; and

"(viii) in complying with the requirements imposed on the Secretary under part C of title XI of the Social Security Act;

"(B) shall study the issues related to the adoption of uniform data standards for patient medical record information and the electronic exchange of such information;

"(C) shall report to the Secretary not later than 4 years after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996 recommendations and legislative proposals for such standards and electronic exchange; and

"(D) shall be responsible generally for advising the Secretary and the Congress on the status of the implementation of part C of title XI of the Social Security Act."; and

(5) by adding at the end the following:

"(7) Not later than 1 year after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, and annually thereafter, the Committee shall submit to the Congress, and make public, a report regarding the implementation of part C of title XI of the Social Security Act. Such report shall address the following subjects, to the extent that the Committee determines appropriate:

"(A) The extent to which persons required to comply with part C of title XI of the Social Security Act are cooperating in implementing the standards adopted under such part.

"(B) The extent to which such entities are meeting the security standards adopted under such part and the types of penalties assessed for noncompliance with such standards.

"(C) Whether the Federal and State Governments are receiving information of sufficient quality to meet their responsibilities under such part.

"(D) Any problems that exist with respect to implementation of such part.

"(E) The extent to which timetables under such part are being met.".

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(a) IN GENERAL.--Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) SUBJECTS FOR RECOMMENDATIONS.--The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

(c) REGULATIONS.--

(1) IN GENERAL.--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).

(2) PREEMPTION.--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.

(d) CONSULTATION.--In carrying out this section, the Secretary of Health and Human Services shall consult with--

(1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and

(2) the Attorney General.

...

Comments/suggestions and other questions about HIPAA should be directed to the Web Master.

Attachment J.16.2

[Federal Register: December 28, 2000 (Volume 65, Number 250)]

[Rules and Regulations]

[Page 82461-82510]

[DOCID:fr28de00-29]

BILLING CODE: 4150-04M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 through 164

Rin: 0991-AB08

Standards for Privacy of Individually Identifiable Health Information

AGENCY: Office of the Assistant Secretary for Planning and Evaluation, DHHS.

ACTION: Final rule.

SUMMARY: This rule includes standards to protect the privacy of individually identifiable health information. The rules below, which apply to health plans, health care clearinghouses, and certain health care providers, present standards with respect to the rights of individuals who are the subjects of this information, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.

The use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors. This rule implements the

privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996.

DATES: The final rule is effective on February 26, 2001.

FOR FURTHER INFORMATION CONTACT: Kimberly Coleman, 1-866-OCR-PRIV (1-866-627-7748) or TTY 1-866-788-4989.

SUPPLEMENTARY INFORMATION:

Availability of copies, and electronic access.

Copies: To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512-1800 or by fax to (202) 512-2250. The cost for each copy is $8.00. As an alternative, you can view and photocopy the **Federal Register** document at most libraries designated as Federal Depository Libraries and at many other public and academic libraries throughout the country that receive the **Federal Register**.

Electronic Access: This document is available electronically at http://aspe.hhs.gov/admnsimp/ as well as at the web site of the Government Printing Office at http://www.access.gpo.gov/su_docs/aces/ aces140.html.

I. BACKGROUND

Table of Contents

§ 160.101 Statutory basis and purpose.

§ 160.102 Applicability.

§ 160.103 Definitions.

§ 160.104 Modifications.

§ 160.201 Applicability

Attachment J.16.2

§ 160.202 Definitions.

§ 160.203 General rule and exceptions.

§ 160.204 Process for requesting exception determinations.

§ 160.205 Duration of effectiveness of exception determinations.

§ 160.300 Applicability.

§ 160.302 Definitions.

§ 160.304 Principles for achieving compliance.

(a) Cooperation.

(b) Assistance.

§ 160.306 Complaints to the Secretary.

(a) Right to file a complaint.

(b) Requirements for filing complaints.

(c) Investigation.

§ 160.308 Compliance reviews.

§ 160.310 Responsibilities of covered entities.

(a) Provide records and compliance reports.

(b) Cooperate with complaint investigations and compliance reviews.

(c) Permit access to information.

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) Resolution where noncompliance is indicated.

(b) Resolution when no violation is found.

§ 164.102 Statutory basis.

§ 164.104 Applicability.

Attachment J.16.2

§ 164.106 Relationship to other parts.

§ 164.500 Applicability.

§ 164.501 Definitions.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) Standard.

(b) Standard: minimum necessary.

(c) Standard: uses and disclosures of protected health information subject to an agreed upon restriction.

(d) Standard: uses and disclosures of de-identified protected health information.

(e) Standard: disclosures to business associates.

(f) Standard: deceased individuals.

(g) Standard: personal representatives.

(h) Standard: confidential communications.

(i) Standard: uses and disclosures consistent with notice.

(j) Standard: disclosures by whistleblowers and workforce member crime victims.

§ 164.504 Uses and disclosures: organizational requirements.

(a) Definitions.

(b) Standard: health care component.

(c) Implementation specification: application of other provisions.

(d) Standard: affiliated covered entities.

(e) Standard: business associate contracts.

(f) Standard: requirements for group health plans.

(g) Standard: requirements for a covered entity with multiple covered functions.

Attachment J.16.2

§ 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations.

(a) Standard: consent requirement.

(b) Implementation specifications: general requirements.

(c) Implementation specifications: content requirements.

(d) Implementation specifications: defective consents.

(e) Standard: resolving conflicting consents and authorizations.

(f) Standard: joint consents.

§164.508 Uses and disclosures for which an authorization is required.

(a) Standard: authorizations for uses and disclosures.

(b) Implementation specifications: general requirements.

(c) Implementation specifications: core elements and requirements.

(d) Implementation specifications: authorizations requested by a covered entity for its own uses and disclosures.

(e) Implementation specifications: authorizations requested by a covered entity for disclosures by others.

(f) Implementation specifications: authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

(a) Standard: use and disclosure for facility directories.

(b) Standard: uses and disclosures for involvement in the individual's care and notification purposes.

§ 164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required.

(a) Standard: uses and disclosures required by law.

(b) Standard: uses and disclosures for public health activities.

(c) Standard: disclosures about victims of abuse, neglect or domestic violence.

(d) Standard: uses and disclosures for health oversight activities.

(e) Standard: disclosures for judicial and administrative proceedings.

(f) Standard: disclosures for law enforcement purposes.

(g) Standard: uses and disclosures about decedents.

(h) Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes.

(i) Standard: uses and disclosures for research purposes.

(j) Standard: uses and disclosures to avert a serious threat to health or safety.

(k) Standard: uses and disclosures for specialized government functions.

(l) Standard: disclosures for workers' compensation.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) Standard: de-identification of protected health information.

(b) Implementation specifications: requirements for de-identification of protected health information.

(c) Implementation specifications: re-identification.

(d) Standard: minimum necessary requirements.

(e) Standard: uses and disclosures of protected health information for marketing.

(f) Standard: uses and disclosures for fundraising.

(g) Standard: uses and disclosures for underwriting and related purposes.

(h) Standard: verification requirements

§ 164.520 Notice of privacy practices for protected health information.

(a) Standard: notice of privacy practices.

(b) Implementation specifications: content of notice.

(c) Implementation specifications: provision of notice.

(d) Implementation specifications: joint notice by separate covered entities.

(e) Implementation specifications: documentation.

§ 164.522 Rights to request privacy protection for protected health information.

(a) Standard: right of an individual to request restriction of uses and disclosures.

(b) Standard: confidential communications requirements.

§ 164.524 Access of individuals to protected health information.

(a) Standard: access to protected health information.

(b) Implementation specifications: requests for access and timely action.

(c) Implementation specifications: provision of access.

(d) Implementation specifications: denial of access.

(e) Implementation specification: documentation.

§ 164.526 Amendment of protected health information.

(a) Standard: right to amend.

(b) Implementation specifications: requests for amendment and timely action.

(c) Implementation specifications: accepting the amendment.

(d) Implementation specifications: denying the amendment.

(e) Implementation specification: actions on notices of amendment.

(f) Implementation specification: documentation.

§ 164.528 Accounting of disclosures of protected health information.

(a) Standard: right to an accounting of disclosures of protected health information.

(b) Implementation specifications: content of the accounting.

(c) Implementation specifications: provision of the accounting.

(d) Implementation specification: documentation.

§ 164.530 Administrative requirements.

(a) Standard: personnel designations.

(b) Standard: training.

(c) Standard: safeguards.

(d) Standard: complaints to the covered entity.

(e) Standard: sanctions

(f) Standard: mitigation.

(g) Standard: refraining from intimidating or retaliatory acts.

(h) Standard: waiver of rights.

(i) Standard: policies and procedures.

(j) Standard: documentation.

(k) Standard: group health plans.

§ 164.532 Transition provisions.

(a) Standard: effect of prior consents and authorizations.

(b) Implementation specification: requirements for retaining effectiveness of prior consents and authorizations.

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) Health care providers.

(b) Health plans.

(c) Health care clearinghouses.

Purpose of the Administrative Simplification Regulations

This regulation has three major purposes:

1. to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information;
2. to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and
3. to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

This regulation is the second final regulation to be issued in the package of rules mandated under Title II Subtitle F Section 261-264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, titled "Administrative Simplification." Congress called for steps to improve "the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." To achieve that end, Congress required the Department to promulgate a set of interlocking regulations establishing standards and protections for health information systems. The first regulation in this set, Standards for Electronic Transactions 65 FR 50312, was published on August 17, 2000 (the "Transactions Rule"). This regulation establishing Standards for Privacy of Individually Identifiable Health Information is the second final rule in the package. A rule establishing a unique identifier for employers to use in electronic health care transactions, a rule establishing a unique identifier for providers for such transactions, and a rule establishing standards for the security of electronic information systems have been proposed. See 63 FR 25272 and 25320 (May 7, 1998); 63 FR 32784 (June 16, 1998); 63 FR 43242 (August 12, 1998). Still to be proposed are rules establishing a unique identifier for health plans for electronic transactions, standards for claims attachments, and standards for transferring among health plans appropriate standard data elements needed for coordination of benefits. (See section C, below, for a more detailed explanation of the statutory mandate for these regulations.)

In enacting HIPAA, Congress recognized the fact that administrative simplification cannot succeed if we do not also protect the privacy and confidentiality of personal health information. The provision of high-quality health care requires the exchange of personal, often-sensitive information between an individual and a skilled practitioner. Vital to that interaction is the patient's ability to trust that the information shared will be protected and kept confidential. Yet many patients are concerned that their information is not protected. Among the factors adding to this concern are the growth of the number of organizations involved in the provision of care and the processing of claims, the growing use of electronic information technology, increased efforts to market health care and other products to consumers, and the increasing ability to collect highly sensitive information about a person's current and future health status as a result of advances in scientific research.

Rules requiring the protection of health privacy in the United States have been enacted primarily by the states. While virtually every state has enacted one or more laws to

safeguard privacy, these laws vary significantly from state to state and typically apply to only part of the health care system. Many states have adopted laws that protect the health information relating to certain health conditions such as mental illness, communicable diseases, cancer, HIV/AIDS, and other stigmatized conditions. An examination of state health privacy laws and regulations, however, found that "state laws, with a few notable exceptions, do not extend comprehensive protections to people's medical records." Many state rules fail to provide such basic protections as ensuring a patient's legal right to see a copy of his or her medical record. See Health Privacy Project, "The State of Health Privacy: An Uneven Terrain," Institute for Health Care Research and Policy, Georgetown University (July 1999) (http://www.healthprivacy.org) (the "Georgetown Study").

Until now, virtually no federal rules existed to protect the privacy of health information and guarantee patient access to such information. This final rule establishes, for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care. The rule sets a floor of ground rules for health care providers, health plans, and health care clearinghouses to follow, in order to protect patients and encourage them to seek needed care. The rule seeks to balance the needs of the individual with the needs of the society. It creates a framework of protection that can be strengthened by both the federal government and by states as health information systems continue to evolve.

Need for a National Health Privacy Framework

The Importance of Privacy

Privacy is a fundamental right. As such, it must be viewed differently than any ordinary economic good. The costs and benefits of a regulation must, of course, be considered as a means of identifying and weighing options. At the same time, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom.

A right to privacy in personal information has historically found expression in American law. All fifty states today recognize in tort law a common law or statutory right to privacy. Many states specifically provide a remedy for public revelation of private facts. Some states, such as California and Tennessee, have a right to privacy as a matter of state constitutional law. The multiple historical sources for legal rights to privacy are traced in many places, including Chapter 13 of Alan Westin's *Privacy and Freedom* and in Ellen Alderman & Caroline Kennedy, *The Right to Privacy* (1995).

Throughout our nation's history, we have placed the rights of the individual at the forefront of our democracy. In the Declaration of Independence, we asserted the "unalienable right" to "life, liberty and the pursuit of happiness." Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against the larger social purposes of the nation.

To take but one example, the Fourth Amendment to the United States Constitution guarantees that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." By referring to the need for security of "persons" as well as "papers and effects" the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of "persons" is consistent with obtaining patient consent before performing invasive medical procedures. The need for security in "papers and effects" underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere. As is generally true for the right of privacy in information, the right is not absolute. The test instead is what constitutes an "unreasonable" search of the papers and effects.

The United States Supreme Court has upheld the constitutional protection of personal health information. In *Whalen v. Roe*, 429 U.S. 589 (1977), the Court analyzed a New York statute that created a database of persons who obtained drugs for which there was both a lawful and unlawful market. The Court, in upholding the statute, recognized at least two different kinds of interests within the constitutionally protected "zone of privacy." "One is the individual interest in avoiding disclosure of personal matters," such as this regulation principally addresses. This interest in avoiding disclosure, discussed in *Whalen* in the context of medical information, was found to be distinct from a different line of cases concerning "the interest in independence in making certain kinds of important decisions."

Individuals' right to privacy in information about themselves is not absolute. It does not, for instance, prevent reporting of public health information on communicable diseases or stop law enforcement from getting information when due process has been observed. But many people believe that individuals should have some right to control personal and sensitive information about themselves. Among different sorts of personal information, health information is among the most sensitive. Many people believe that details about their physical self should not generally be put on display for neighbors, employers, and government officials to see. Informed consent laws place limits on the ability of other persons to intrude physically on a person's body. Similar concerns apply to intrusions on information about the person.

Moving beyond these facts of physical treatment, there is also significant intrusion when records reveal details about a person's mental state, such as during treatment for mental health. If, in Justice Brandeis' words, the "right to be let alone" means anything, then it likely applies to having outsiders have access to one's intimate thoughts, words, and emotions. In the recent case of *Jaffee v. Redmond*, 116 S.Ct. 1923 (1996), the Supreme Court held that statements made to a therapist during a counseling session were protected against civil discovery under the Federal Rules of Evidence. The Court noted that all fifty states have adopted some form of the psychotherapist-patient privilege. In upholding the federal privilege, the Supreme Court stated that it "serves the public interest by facilitating the appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance."

Many writers have urged a philosophical or common-sense right to privacy in one's personal information. Examples include Alan Westin, *Privacy and Freedom* (1967) and Janna Malamud Smith, *Private Matters: In Defense of the Personal Life* (1997). These writings emphasize the link between privacy and freedom and privacy and the "personal life," or the ability to develop one's own personality and self-expression. Smith, for instance, states:

The bottom line is clear. If we continually, gratuitously, reveal other people's privacies, we harm them and ourselves, we undermine the richness of the personal life, and we fuel a social atmosphere of mutual exploitation. Let me put it another way: Little in life is as precious as the freedom to say and do things with people you love that you would not say or do if someone else were present. And few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material. Id. at 240-241.

In 1890, Louis D. Brandeis and Samuel D. Warren defined the right to privacy as "the right to be let alone." See L. Brandeis, S. Warren, "The Right To Privacy," 4 Harv.L.Rev. 193. More than a century later, privacy continues to play an important role in Americans' lives. In their book, *The Right to Privacy*, (Alfred A. Knopf, New York, 1995) Ellen Alderman and Caroline Kennedy describe the importance of privacy in this way:

Privacy covers many things. It protects the solitude necessary for creative thought. It allows us the independence that is part of raising a family. It protects our right to be secure in our own homes and possessions, assured that the government cannot come barging in. Privacy also encompasses our right to self-determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized.

Or, as Cavoukian and Tapscott observed the right of privacy is: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated." See A. Cavoukian, D. Tapscott, "Who Knows: Safeguarding Your Privacy in a Networked World," Random House (1995).

Increasing Public Concern About Loss of Privacy

Today, it is virtually impossible for any person to be truly "let alone." The average American is inundated with requests for information from potential employers, retail shops, telephone marketing firms, electronic marketers, banks, insurance companies, hospitals, physicians, health plans, and others. In a 1998 national survey, 88 percent of consumers said they were "concerned" by the amount of information being requested, including 55 percent who said they were "very concerned." See Privacy and American Business, *1998 Privacy Concerns & Consumer Choice Survey* (http://www.pandab.org) These worries are not just theoretical. Consumers who use the Internet to make purchases or request "free" information often are asked for personal and financial information. Companies making such requests routinely promise to protect the confidentiality of that

information. Yet several firms have tried to sell this information to other companies even after promising not to do so.

Americans' concern about the privacy of their health information is part of a broader anxiety about their lack of privacy in an array of areas. A series of national public opinion polls conducted by Louis Harris & Associates documents a rising level of public concern about privacy, growing from 64 percent in 1978 to 82 percent in 1995. Over 80 percent of persons surveyed in 1999 agreed with the statement that they had "lost all control over their personal information." See Harris Equifax, *Health Information Privacy Study* (1993) (http://www.epic.org/privacy/medical/polls.html). A Wall Street Journal/ABC poll on September 16, 1999 asked Americans what concerned them most in the coming century. "Loss of personal privacy" was the first or second concern of 29 percent of respondents. All other issues, such a terrorism, world war, and global warming had scores of 23 percent or less.

This growing concern stems from several trends, including the growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and, in health care, the increasing complexity of the system. Each of these trends brings the potential for tremendous benefits to individuals and society generally. At the same time, each also brings new potential for invasions of our privacy.

Increasing Use of Interconnected Electronic Information Systems

Until recently, health information was recorded and maintained on paper and stored in the offices of community-based physicians, nurses, hospitals, and other health care professionals and institutions. In some ways, this imperfect system of record keeping created a false sense of privacy among patients, providers, and others. Patients' health information has never remained completely confidential. Until recently, however, a breach of confidentiality involved a physical exchange of paper records or a verbal exchange of information. Today, however, more and more health care providers, plans, and others are utilizing electronic means of storing and transmitting health information. In 1996, the health care industry invested an estimated $10 billion to $15 billion on information technology. See National Research Council, Computer Science and Telecommunications Board, "For the Record: Protecting Electronic Health Information," (1997). The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time. While the majority of medical records still are in paper form, information from those records is often copied and transmitted through electronic means.

This ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology affords many benefits to individuals and to the health care industry. Use of electronic information has helped to speed the delivery of effective care and the processing of billions of dollars worth of

health care claims. Greater use of electronic data has also increased our ability to identify and treat those who are at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve the quality of care delivered in the U.S. The National Research Council recently reported that "the Internet has great potential to improve Americans' health by enhancing communications and improving access to information for care providers, patients, health plan administrators, public health officials, biomedical researchers, and other health professionals." See "Networking Health: Prescriptions for the Internet," National Academy of Sciences (2000).

At the same time, these advances have reduced or eliminated many of the financial and logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals. And they have made our information available to many more people. The shift from paper to electronic records, with the accompanying greater flows of sensitive health information, thus strengthens the arguments for giving legal protection to the right to privacy in health information. In an earlier period where it was far more expensive to access and use medical records, the risk of harm to individuals was relatively low. In the potential near future, when technology makes it almost free to send lifetime medical records over the Internet, the risks may grow rapidly. It may become cost-effective, for instance, for companies to offer services that allow purchasers to obtain details of a person's physical and mental treatments. In addition to legitimate possible uses for such services, malicious or inquisitive persons may download medical records for purposes ranging from identity theft to embarrassment to prurient interest in the life of a celebrity or neighbor. The comments to the proposed privacy rule indicate that many persons believe that they have a right to live in society without having these details of their lives laid open to unknown and possibly hostile eyes. These technological changes, in short, may provide a reason for institutionalizing privacy protections in situations where the risk of harm did not previously justify writing such protections into law.

The growing level of trepidation about privacy in general, noted above, has tracked the rise in electronic information technology. Americans have embraced the use of the Internet and other forms of electronic information as a way to provide greater access to information, save time, and save money. For example, 60 percent of Americans surveyed in 1999 reported that they have a computer in their home; 82 percent reported that they have used a computer; 64 percent say they have used the Internet; and 58 percent have sent an e-mail. Among those who are under the age of 60, these percentages are even higher. See "National Survey of Adults on Technology," Henry J. Kaiser Family Foundation (February, 2000). But 59 percent of Americans reported that they worry that an unauthorized person will gain access to their information. A recent survey suggests that 75 percent of consumers seeking health information on the Internet are concerned or very concerned about the health sites they visit sharing their personal health information with a third party without their permission. Ethics Survey of Consumer Attitudes about Health Web Sites, California Health Care Foundation, at 3 (January, 2000).

Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health

information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data. Many plans, providers, and clearinghouses have taken steps to safeguard the privacy of individually identifiable health information. Yet they must currently rely on a patchwork of State laws and regulations that are incomplete and, at times, inconsistent. States have, to varying degrees, attempted to enhance confidentiality by establishing laws governing at least some aspects of medical record privacy. This approach, though a step in the right direction, is inadequate. These laws fail to provide a consistent or comprehensive legal foundation of health information privacy. For example, there is considerable variation among the states in the type of information protected and the scope of the protections provided. See Georgetown Study, at Executive Summary; Lawrence O. Gostin, Zita Lazzarrini, Kathleen M. Flaherty, *Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization*, Report to Centers for Disease Control, Council of State and Territorial Epidemiologists, and Task Force for Child Survival and Development, Carter Presidential Center (1996) (Gostin Study).

Moreover, electronic health data is becoming increasingly "national"; as more information becomes available in electronic form, it can have value far beyond the immediate community where the patient resides. Neither private action nor state laws provide a sufficiently comprehensive and rigorous legal structure to allay public concerns, protect the right to privacy, and correct the market failures caused by the absence of privacy protections (see discussion below of market failure under section V.C). Hence, a national policy with consistent rules is necessary to encourage the increased and proper use of electronic information while also protecting the very real needs of patients to safeguard their privacy.

Advances in Genetic Sciences

Recently, scientists completed nearly a decade of work unlocking the mysteries of the human genome, creating tremendous new opportunities to identify and prevent many of the leading causes of death and disability in this country and around the world. Yet the absence of privacy protections for health information endanger these efforts by creating a barrier of distrust and suspicion among consumers. A 1995 national poll found that more than 85 percent of those surveyed were either "very concerned" or "somewhat concerned" that insurers and employers might gain access to and use genetic information. See Harris Poll, 1995 #34. Sixty-three percent of the 1,000 participants in a 1997 national survey said they would not take genetic tests if insurers and employers could gain access to the results. See "Genetic Information and the Workplace," Department of Labor, Department of Health and Human Services, Equal Employment Opportunity Commission, January 20, 1998. "In genetic testing studies at the National Institutes of Health, thirty-two percent of eligible people who were offered a test for breast cancer risk declined to take it, citing concerns about loss of privacy and the potential for discrimination in health insurance." Sen. Leahy's comments for March 10, 1999 Introduction of the Medical Information Privacy and Security Act.

The Changing Health Care System

Attachment J.16.2

The number of entities who are maintaining and transmitting individually identifiable health information has increased significantly over the last 10 years. In addition, the rapid growth of integrated health care delivery systems requires greater use of integrated health information systems. The health care industry has been transformed from one that relied primarily on one-on-one interactions between patients and clinicians to a system of integrated health care delivery networks and managed care providers. Such a system requires the processing and collection of information about patients and plan enrollees (for example, in claims files or enrollment records), resulting in the creation of databases that can be easily transmitted. This dramatic change in the practice of medicine brings with it important prospects for the improvement of the quality of care and reducing the cost of that care. It also, however, means that increasing numbers of people have access to health information. And, as health plan functions are increasingly outsourced, a growing number of organizations not affiliated with our physicians or health plans also have access to health information.

According to the American Health Information Management Association (AHIMA), an average of 150 people "from nursing staff to x-ray technicians, to billing clerks" have access to a patient's medical records during the course of a typical hospitalization. While many of these individuals have a legitimate need to see all or part of a patient's records, no laws govern who those people are, what information they are able to see, and what they are and are not allowed to do with that information once they have access to it. According to the National Research Council, individually identifiable health information frequently is shared with:

- Consulting physicians;
- Managed care organizations;
- Health insurance companies
- Life insurance companies;
- Self-insured employers;
- Pharmacies;
- Pharmacy benefit managers;
- Clinical laboratories;
- Accrediting organizations;
- State and Federal statistical agencies; and
- Medical information bureaus.

Much of this sharing of information is done without the knowledge of the patient involved. While many of these functions are important for smooth functioning of the health care system, there are no rules governing how that information is used by secondary and tertiary users. For example, a pharmacy benefit manager could receive information to determine whether an insurance plan or HMO should cover a prescription, but then use the information to market other products to the same patient. Similarly, many of us obtain health insurance coverage though our employer and, in some instances, the employer itself acts as the insurer. In these cases, the employer will obtain identifiable health information about its employees as part of the legitimate health insurance functions such as claims processing, quality improvement, and fraud detection activities. At the same time, there is no comprehensive protection prohibiting the employer from using that information to make decisions about promotions or job retention.

Public concerns reflect these developments. A 1993 Lou Harris poll found that 75 percent of those surveyed worry that medical information from a computerized national health information system will be used for many non-health reasons, and 38 percent are very concerned. This poll, taken during the health reform efforts of 1993, showed that 85 percent of respondents believed that protecting the confidentiality of medical records is "absolutely essential" or "very essential" in health care reform. An ACLU Poll in 1994 also found that 75 percent of those surveyed are concerned a "great deal" or a "fair amount'" about insurance companies putting medical information about them into a computer information bank to which others have access. Harris Equifax, Health Information Privacy Study 2,33 (1993) http://www.epic.org/privacy/medical/poll.html. Another survey found that 35 percent of Fortune 500 companies look at people's medical records before making hiring and promotion decisions. Starr, Paul. "Health and the Right to Privacy," American Journal of Law and Medicine, 1999. Vol 25, pp. 193-201.

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. In the absence of a national legal framework of health privacy protections, consumers are increasingly vulnerable to the exposure of their personal health information. Disclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security. Examples of recent privacy breaches include:

• A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).

• A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).

• An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).

• The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).

• A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).

• A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).

• A speculator bid $4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (New York Times, August 14, 1991).

• In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).

• A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997).

No matter how or why a disclosure of personal information is made, the harm to the individual is the same. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care system.

Privacy is Necessary to Secure Effective, High Quality Health Care

While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the effective delivery of health care, both to individuals and to populations. The market failures caused by the lack of effective privacy protections for health information are discussed below (see section V.C below). Here, we discuss how privacy is a necessary foundation for delivery of high quality health care. In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers.

The need for privacy of health information, in particular, has long been recognized as critical to the delivery of needed medical care. More than anything else, the relationship between a patient and a clinician is based on trust. The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and to

respect the need to keep such information private. In order to receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives. The provision of health information assists in the diagnosis of an illness or condition, in the development of a treatment plan, and in the evaluation of the effectiveness of that treatment. In the absence of full and accurate information, there is a serious risk that the treatment plan will be inappropriate to the patient's situation.

Patients also benefit from the disclosure of such information to the health plans that pay for and can help them gain access to needed care. Health plans and health care clearinghouses rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to receive needed care, the quality of that care, and the efficiency with which it is delivered.

Accurate medical records assist communities in identifying troubling public health trends and in evaluating the effectiveness of various public health efforts. Accurate information helps public and private payers make correct payments for care received and lower costs by identifying fraud. Accurate information provides scientists with data they need to conduct research. We cannot improve the quality of health care without information about which treatments work, and which do not.

Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions.

Patients who are worried about the possible misuse of their information often take steps to protect their privacy. Recent studies show that a person who does not believe his privacy will be protected is much less likely to participate fully in the diagnosis and treatment of his medical condition. A national survey conducted in January 1999 found that one in five Americans believe their health information is being used inappropriately. See California HealthCare Foundation, "National Survey: Confidentiality of Medical Records"(January, 1999) (http://www.chcf.org). More troubling is the fact that one in six Americans reported that they have taken some sort of evasive action to avoid the inappropriate use of their information by providing inaccurate information to a health care provider, changing physicians, or avoiding care altogether. Similarly, in its comments on our proposed rule, the Association of American Physicians and Surgeons reported 78 percent of its members reported withholding information from a patient's record due to privacy concerns and another 87 percent reported having had a patient request to withhold information from their records. For an example of this phenomenon in a particular demographic group, see Drs. Bearman, Ford, and Moody, "Foregone Health Care among Adolescents," *JAMA*, vol. 282, no. 23 (999); Cheng, T.L., et al., "Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes among High School Students," *JAMA*, vol. 269, no. 11 (1993), at 1404-1407.

The absence of strong national standards for medical privacy has widespread consequences. Health care professionals who lose the trust of their patients cannot deliver high-quality care. In 1999, a coalition of organizations representing various stakeholders including health plans, physicians, nurses, employers, disability and mental health advocates, accreditation organizations as well as experts in public health, medical ethics, information systems, and health policy adopted a set of "best principles" for health care privacy that are consistent with the standards we lay out here. (See the Health Privacy Working Group, "Best Principles for Health Privacy" (July, 1999) (Best Principles Study). The Best Principles Study states that -

To protect their privacy and avoid embarrassment, stigma, and discrimination, some people withhold information from their health care providers, provide inaccurate information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and - in some cases - avoid care altogether.

Best Principles Study, at 9. In their comments on our proposed rule, numerous organizations representing health plans, health providers, employers, and others acknowledged the value of a set of national privacy standards to the efficient operation of their practices and businesses.

Breaches of Health Privacy Harm More than Our Health Status

A breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. For example:

• A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages. See the National Law Journal, May 30, 1994.

• A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended. See *Estate of Behringer v. Medical Center at Princeton*, 249 N.J. Super. 597.

• A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See *New York Times*, October 10, 1992, Section 1, page 25.

• A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression. (Los Angeles Times, September 1, 1998)

• Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission. "Who's reading your Medical Records," Consumer Reports, October 1994, at 628, paraphrasing Sweeny, Latanya, "Weaving Technology and Policy Together to Maintain

Confidentiality," The Journal Of Law Medicine and Ethics (Summer & Fall 1997) Vol. 25, Numbers 2,3.

The answer to these concerns is not for consumers to withdraw from society and the health care system, but for society to establish a clear national legal framework for privacy. By spelling out what is and what is not an allowable use of a person's identifiable health information, such standards can help to restore and preserve trust in the health care system and the individuals and institutions that comprise that system. As medical historian Paul Starr wrote: "Patients have a strong interest in preserving the privacy of their personal health information but they also have an interest in medical research and other efforts by health care organizations to improve the medical care they receive. As members of the wider community, they have an interest in public health measures that require the collection of personal data." (P. Starr, "Health and the Right to Privacy," American Journal of Law & Medicine, 25, nos. 2&3 (1999) 193-201). The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole.

National standards for medical privacy must recognize the sometimes competing goals of improving individual and public health, advancing scientific knowledge, enforcing the laws of the land, and processing and paying claims for health care services. This need for balance has been recognized by many of the experts in this field. Cavoukian and Tapscott described it this way: "An individual's right to privacy may conflict with the collective rights of the public. . .We do not suggest that privacy is an absolute right that reigns supreme over all other rights. It does not. However, the case for privacy will depend on a number of factors that can influence the balance - the level of harm to the individual involved versus the needs of the public."

The Federal Response

There have been numerous federal initiatives aimed at protecting the privacy of especially sensitive personal information over the past several years -- and several decades. While the rules below are likely the largest single federal initiative to protect privacy, they are by no means alone in the field. Rather, the rules arrive in the context of recent legislative activity to grapple with advances in technology, in addition to an already established body of law granting federal protections for personal privacy.

In 1965, the House of Representatives created a Special Subcommittee on Invasion of Privacy. In 1973, this Department's predecessor agency, the Department of Health, Education and Welfare issued *The Code of Fair Information Practice Principles* establishing an important baseline for information privacy in the U.S. These principles formed the basis for the federal Privacy Act of 1974, which regulates the government's use of personal information by limiting the disclosure of personally-identifiable information, allows consumers access to information about them, requires federal agencies to specify the purposes for collecting personal information, and provides civil and criminal penalties for misuse of information.

In the last several years, with the rapid expansion in electronic technology -- and accompanying concerns about individual privacy -- laws, regulations, and legislative proposals have been developed in areas ranging from financial privacy to genetic privacy to the safeguarding of children on-line. For example, the Children's Online Privacy Protection Act was enacted in 1998, providing protection for children when interacting at web-sites. In February, 2000, President Clinton signed Executive Order 13145, banning the use of genetic information in federal hiring and promotion decisions. The landmark financial modernization bill, signed by the President in November, 1999, likewise contained financial privacy protections for consumers. There also has been recent legislative activity on establishing legal safeguards for the privacy of individuals' Social Security numbers, and calls for regulation of on-line privacy in general.

These most recent laws, regulations, and legislative proposals come against the backdrop of decades of privacy-enhancing statutes passed at the federal level to enact safeguards in fields ranging from government data files to video rental records. In the 1970s, individual privacy was paramount in the passage of the Fair Credit Reporting Act (1970), the Privacy Act (1974), the Family Educational Rights and Privacy Act (1974), and the Right to Financial Privacy Act (1978). These key laws were followed in the next decade by another series of statutes, including the Privacy Protection Act (1980), the Electronic Communications Privacy Act (1986), the Video Privacy Protection Act (1988), and the Employee Polygraph Protection Act (1988). In the last ten years, Congress and the President have passed additional legal privacy protection through, among others, the Telephone Consumer Protection Act (1991), the Driver's Privacy Protection Act (1994), the Telecommunications Act (1996), the Children's Online Privacy Protection Act (1998), the Identity Theft and Assumption Deterrence Act (1998), and Title V of the Gramm-Leach-Bliley Act (1999) governing financial privacy.

In 1997, a Presidential advisory commission, the Advisory Commission on Consumer Protection and Quality in the Health Care Industry, recognized the need for patient privacy protection in its recommendations for a Consumer Bill of Rights and Responsibilities (November 1997). In 1997, Congress enacted the Balanced Budget Act (Public Law 105-34), which added language to the Social Security Act (18 U.S.C. 1852) to require Medicare+Choice organizations to establish safeguards for the privacy of individually identifiable patient information. Similarly, the Veterans Benefits section of the U.S. Code provides for confidentiality of medical records in cases involving drug abuse, alcoholism or alcohol abuse, HIV infection, or sickle cell anemia (38 U.S.C. 7332).

As described in more detail in the next section, Congress recognized the importance of protecting the privacy of health information by enacting the Health Insurance Portability and Accountability Act of 1996. The Act called on Congress to enact a medical privacy statute and asked the Secretary of Health and Human Services to provide Congress with recommendations for protecting the confidentiality of health care information. The Congress further recognized the importance of such standards by providing the Secretary with authority to promulgate regulations on health care privacy in the event that lawmakers were unable to act within the allotted three years.

Finally, it also is important for the U.S. to join the rest of the developed world in establishing basic medical privacy protections. In 1995, the European Union (EU) adopted a Data Privacy Directive requiring its 15 member states to adopt consistent privacy laws by October 1998. The EU urged all other nations to do the same or face the potential loss of access to information from EU countries.

Statutory Background

History of the Privacy Component of the Administrative Simplification Provisions

The Congress addressed the opportunities and challenges presented by the rapid evolution of health information systems in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which was enacted on August 21, 1996. Sections 261 through 264 of HIPAA are known as the Administrative Simplification provisions. The major part of these Administrative Simplification provisions are found at section 262 of HIPAA, which enacted a new part C of title XI of the Social Security Act (hereinafter we refer to the Social Security Act as the "Act" and we refer to all other laws cited in this document by their names).

In section 262, Congress primarily sought to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords. Thus, section 262 directs HHS to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions.

At the same time, Congress recognized the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in health information systems technology and communications. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of health information.

Congress has long recognized the need for protection of health information privacy generally, as well as the privacy implications of electronic data interchange and the increased ease of transmitting and sharing individually identifiable health information. Congress has been working on broad health privacy legislation for many years and, as evidenced by the self-imposed three year deadline included in the HIPAA, discussed below, believes it can and should enact such legislation. A significant portion of the first Administrative Simplification section debated on the floor of the Senate in 1994 (as part of the Health Security Act) consisted of privacy provisions. In the version of the HIPAA passed by the House of Representatives in 1996, the requirement for the issuance of privacy standards was located in the same section of the bill (section 1173) as the requirements for issuance of the other HIPAA Administrative Simplification standards. In conference, the requirement for privacy standards was moved to a separate section in the same part of HIPAA, section 264, so that Congress could link the Privacy standards to Congressional action.

Section 264(b) requires the Secretary of HHS to develop and submit to the Congress recommendations for:

• The rights that an individual who is a subject of individually identifiable health information should have.

• The procedures that should be established for the exercise of such rights.

• The uses and disclosures of such information that should be authorized or required.

The Secretary's Recommendations were submitted to the Congress on September 11, 1997. Section 264(c)(1) provides that:

If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than [February 21, 2000]. Such regulations shall address at least the subjects described in subsection (b).

As the Congress did not enact legislation regarding the privacy of individually identifiable health information prior to August 21, 1999, HHS published proposed rules setting forth such standards on November 3, 1999, 64 FR 59918, and is now publishing the mandated final regulation.

These privacy standards have been, and continue to be, an integral part of the suite of Administrative Simplification standards intended to simplify and improve the efficiency of the administration of our health care system.

The Administrative Simplification Provisions, and Regulatory Actions To Date

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and health care providers who conduct the identified transactions electronically.

The first section, section 1171 of the Act, establishes definitions for purposes of part C of title XI for the following terms: code set, health care clearinghouse, health care provider, health information, health plan, individually identifiable health information, standard, and standard setting organization.

Section 1172 of the Act makes the standard adopted under part C applicable to: (1) health plans, (2) health care clearinghouses, and (3) health care providers who transmit health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (hereinafter referred to as the "covered entities"). Section 1172 also contains procedural requirements concerning the adoption of standards, including the role

of standard setting organizations and required consultations, summarized in subsection F and section VI, below.

Section 1173 of the Act requires the Secretary to adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically. Section 1173(a)(1) describes the transactions to be promulgated, which include the nine transactions listed in section 1173(a)(2) and other transactions determined appropriate by the Secretary. The remainder of section 1173 sets out requirements for the specific standards the Secretary is to adopt: unique health identifiers, code sets, security standards, electronic signatures, and transfer of information among health plans. Of particular relevance to this proposed rule is section 1173(d), the security standard provision. The security standard authority applies to both the transmission and the maintenance of health information, and requires the entities described in section 1172(a) to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the information, protect against reasonably anticipated threats or hazards to the security or integrity of the information or unauthorized uses or disclosures of the information, and to ensure compliance with part C by the entity's officers and employees.

In section 1174 of the Act, the Secretary is required to establish standards for all of the above transactions, except claims attachments, by February 21, 1998. The statutory deadline for the claims attachment standard is February 21, 1999.

As noted above, a proposed rule for most of the transactions was published on May 7, 1998, and the final Transactions Rule was promulgated on August 17, 2000. The delay was caused by the deliberate consensus building process, working with industry, and the large number of comments received (about 17,000). In addition, in a series of Notices of Proposed Rulemakings, HHS published other proposed standards, as described above. Each of these steps was taken in concert with the affected professions and industries, to ensure rapid adoption and compliance.

Generally, after a standard is established, it may not be changed during the first year after adoption except for changes that are necessary to permit compliance with the standard. Modifications to any of these standards may be made after the first year, but not more frequently than once every 12 months. The Secretary also must ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets and that there are crosswalks from prior versions.

Section 1175 of the Act prohibits health plans from refusing to process, or from delaying processing of, a transaction that is presented in standard format. It also establishes a timetable for compliance: each person to whom a standard or implementation specification applies is required to comply with the standard within 24 months (or 36 months for small health plans) of its adoption. A health plan or other entity may, of course, comply voluntarily before the effective date. The section also provides that compliance with modifications to standards or implementation specifications must be

accomplished by a date designated by the Secretary, which date may not be earlier than 180 days from the notice of change.

Section 1176 of the Act establishes civil monetary penalties for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year. The procedural provisions of section 1128A of the Act apply to actions taken to obtain civil monetary penalties under this section.

Section 1177 establishes penalties for any person that knowingly uses a unique health identifier, or obtains or discloses individually identifiable health information in violation of the part. The penalties include: (1) a fine of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if the offense is "under false pretenses," a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years.

Under section 1178 of the Act, the requirements of part C, as well as any standards or implementation specifications adopted thereunder, preempt contrary state law. There are three exceptions to this general rule of preemption: state laws that the Secretary determines are necessary for certain purposes set forth in the statute; state laws that the Secretary determines address controlled substances; and state laws relating to the privacy of individually identifiable health information that are contrary to and more stringent than the federal requirements. There also are certain areas of state law (generally relating to public health and oversight of health plans) that are explicitly carved out of the general rule of preemption and addressed separately.

Section 1179 of the Act makes the above provisions inapplicable to financial institutions (as defined by section 1101 of the Right to Financial Privacy Act of 1978) or anyone acting on behalf of a financial institution when "authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution."

Finally, as explained above, section 264 requires the Secretary to issue standards with respect to the privacy of individually identifiable health information. Section 264 also contains a preemption provision that provides that contrary provisions of state laws that are more stringent than the federal standards, requirements, or implementation specifications will not be preempted.

Our Approach to This Regulation

Balance

A number of facts informed our approach to this regulation. Determining the best approach to protecting privacy depends on where we start, both with respect to existing legal expectations and also with respect to the expectations of individuals, health care providers, payers and other stakeholders. From the comments we received on the proposed rule, and from the extensive fact finding in which we engaged, a confused picture developed. We learned that stakeholders in the system have very different ideas about the extent and nature of the privacy protections that exist today, and very different ideas about appropriate uses of health information. This leads us to seek to balance the views of the different stakeholders, weighing the varying interests on each particular issue with a view to creating balance in the regulation as a whole.

For example, we received hundreds of comments explaining the legitimacy of various uses and disclosure of health information. We agree that many uses and disclosures of health information are "legitimate," but that is not the end of the inquiry. Neither privacy, nor the important social goals described by the commenters, are absolutes. In this regulation, we are asking health providers and institutions to add privacy into the balance, and we are asking individuals to add social goals into the balance.

The vast difference among regulated entities also informed our approach in significant ways. This regulation applies to solo practitioners, and multi-national health plans. It applies to pharmacies and information clearinghouses. These entities differ not only in the nature and scope of their businesses, but also in the degree of sophistication of their information systems and information needs. We therefore designed the core requirements of this regulation to be flexible and "scalable." This is reflected throughout the rule, particularly in the implementation specifications for making the 'minimum necessary' uses and disclosures, and in the administrative policies and procedures requirements.

We also are informed by the rapid evolution in industry organization and practice. Our goal is to enhance privacy protections in ways that do not impede this evolution. For example, we received many comments asking us to assign a status under this regulation based on a label or title. For example, many commenters asked whether "disease management" is a "health care operation," or whether a "pharmacy benefits manager" is a covered entity. From the comments and our fact-finding, however, we learned that these terms do not have consistent meanings today; rather, they encompass diverse activities and information practices. Further, the statutory definitions of key terms such as 'health care provider' and 'health care clearinghouse' describe functions, not specific types of persons or entities. To respect both the Congressional approach and industry evolution, we design the rule to follow activities and functions, not titles and labels.

Similarly, many comments asked whether a particular person would be a "business associate" under the rule, based on the nature of the person's business. Whether a business associate arrangement must exist under the rule, however, depends on the relationship between the entities and the services being performed, not on the type of persons or companies involved.

Our approach is also significantly informed by the limited jurisdiction conferred by HIPAA. In large part, we have the authority to regulate those who create and disclose health information, but not many key stakeholders who receive that health information from a covered entity. Again, this led us to look to the balance between the burden on covered entities and need to protect privacy in determining our approach to such disclosures. In some instances, we approach this dilemma by requiring covered entities to obtain a representation or documentation of purpose from the person requesting information. While there would be advantages to legislation regulating such third persons directly, we cannot justify abandoning any effort to enhance privacy.

It also became clear from the comments and our fact-finding that we have expectations as a society that conflict with individuals' views about the privacy of health information. We expect the health care industry to develop treatment protocols for the delivery of high quality health care. We expect insurers and the government to reduce fraud in the health care system. We expect to be protected from epidemics, and we expect medical research to produce miracles. We expect the police to apprehend suspects, and we expect to pay for our care by credit card. All of these activities involve disclosure of health information to someone other than our physician.

While most commenters support the concept of health privacy in general, many go on to describe activities that depend on the disclosure of health information and urge us to protect those information flows. Section III, in which we respond to the comments, describes our approach to balancing these conflicting expectations.

Finally, we note that many commenters were concerned that this regulation would lessen current privacy protections. It is important to understand this regulation as a new federal floor of privacy protections that does not disturb more protective rules or practices. Nor do we intend this regulation to describe a set of a "best practices." Rather, this regulation describes a set of basic consumer protections and a series of regulatory permissions for use and disclosure of health information. The protections are a mandatory floor, which other governments and any covered entity may exceed. The permissions are just that, permissive -- the only disclosures of health information required under this rule are to the individual who is the subject of the information or to the Secretary for enforcement of this rule. We expect covered entities to rely on their professional ethics and use their own best judgements in deciding which of these permissions they will use.

Combining Workability with New Protections

This rule establishes national minimum standards to protect the privacy of individually identifiable health information in prescribed settings. The standards address the many varied uses and disclosures of individually identifiable health information by health plans, certain health care providers and health care clearinghouses. The complexity of the standards reflects the complexity of the health care marketplace to which they apply and the variety of subjects that must be addressed. The rule applies not only to the core health care functions relating to treating patients and reimbursing health care providers, but also to activities that range from when individually identifiable health information should be

available for research without authorization to whether a health care provider may release protected health information about a patient for law enforcement purposes. The number of discrete provisions, and the number of commenters requesting that the rule recognize particular activities, is evidence of the significant role that individually identifiable health information plays in many vital public and private concerns.

At the same time, the large number of comments from individuals and groups representing individuals demonstrate the deep public concern about the need to protect the privacy of individually identifiable health information. The discussion above is rich with evidence about the importance of protecting privacy and the potential adverse consequences to individuals and their health if such protections are not extended.

The need to balance these competing interests - the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes - in a way that is also workable for the varied stakeholders causes much of the complexity in the rule. Achieving workability without sacrificing protection means some level of complexity, because the rule must track current practices and current practices are complex. We believe that the complexity entailed in reflecting those practices is better public policy than a perhaps simpler rule that disturbed important information flows.

Although the rule taken as a whole is complicated, we believe that the standards are much less complex as they apply to particular actors. What a health plan or covered health care provider must do to comply with the rule is clear, and the two-year delayed implementation provides a substantial period for trade and professional associations, working with their members, to assess the effects of the standards and develop policies and procedures to come into compliance with them. For individuals, the system may look substantially more complicated because, for the first time, we are ensuring that individuals will receive detailed information about how their individually identifiable health information may be used and disclosed. We also provide individuals with additional tools to exercise some control over those uses and disclosures. The additional complexity for individuals is the price of expanding their understanding and their rights.

The Department will work actively with members of the health care industry, representatives of individuals and others during the implementation of this rule. As stated elsewhere, our focus is to develop broader understanding of how the standards work and to facilitate compliance. We intend to provide guidance and check lists as appropriate, particularly to small businesses affected by the rule. We also will work with trade and professional associations to develop guidance and provide technical assistance so that they can help their members understand and comply with these new standards. If this effort is to succeed, the various public and private participants inside and outside of the health care system will need to work together to assure that the competing interests described above remain in balance and that an ethic that recognizes their importance is established.

Enforcement

The Secretary has decided to delegate her responsibility under this regulation to the Department's Office for Civil Rights (OCR). OCR will be responsible for enforcement of this regulation. Enforcement activities will include working with covered entities to secure voluntary compliance through the provision of technical assistance and other means; responding to questions regarding the regulation and providing interpretations and guidance; responding to state requests for exception determinations; investigating complaints and conducting compliance reviews; and, where voluntary compliance cannot be achieved, seeking civil monetary penalties and making referrals for criminal prosecution.

Consent

Current law and practice

The issue that drew the most comments overall is the question of when individuals' permission should be obtained prior to use or disclosure of their health information. We learned that individuals' views and the legal view of 'consent' for use and disclosure of health information are different and in many ways incompatible. Comments from individuals revealed a common belief that, today, people must be asked permission for each and every release of their health information. Many believe that they "own" the health records about them. However, current law and practice do not support this view.

Current privacy protection practices are determined in part by the standards and practices that the professional associations have adopted for their members. Professional codes of conduct for ethical behavior generally can be found as opinions and guidelines developed by organizations such as the American Medical Association, American Nurses' Association, the American Hospital Association, the American Psychiatric Association, and the American Dental Association. These are generally issued though an organization's governing body. The codes do not have the force of law, but providers often recognize them as binding rules.

Our review of professional codes of ethics revealed partial, but loose, support for individuals' expectations of privacy. For example, the American Medical Association's Code of Ethics recognizes both the right to privacy and the need to balance it against societal needs. It reads in part: "conflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of the patient, except where that would result in serious health hazard or harm to the patient or others." AMA Policy No 140.989. See also, Mass. Med. Society, *Patient Privacy and Confidentiality* (1996), at 14:

Patients enter treatment with the expectation that the information they share will be used exclusively for their clinical care. Protection of our patients' confidences is an integral part of our ethical training.

These codes, however, do not apply to many who obtain information from providers. For example, the National Association of Insurance Commissioners model code, "Health Information Privacy Model Act"(1998), applies to insurers but has not been widely

adopted. Codes of ethics are also often written in general terms that do not provide guidance to providers and plans confronted with specific questions about protecting health information.

State laws are a crucial means of protecting health information, and today state laws vary dramatically. Some states defer to the professional codes of conduct, others provide general guidelines for privacy protection, and others provide detailed requirements relating to the protection of information relating to specific diseases or to entire classes of information. Cf., D.C. Code Ann. §2-3305.14(16) and Haw. Rev. Stat. 323C, et seq. In general, state statutes and case law addressing consent to use of health information do not support the public's strong expectations regarding consent for use and disclosure of health information. Only about half of the states have a general law that prohibits disclosure of health information without patient authorization and some of these are limited to hospital medical records.

Even when a state has a law limiting disclosure of health information, the law typically exempts many types of disclosure from the authorization requirement. Georgetown Study, Key Findings; Lisa Dahm, "50-State Survey on Patient Health Care Record Confidentiality," American Health Lawyers Association (1999). One of the most common exemptions from a consent requirement is disclosure of health information for treatment and related purposes. See, e.g., Wis.Stat. § 164.82; Cal. Civ. Code 56:10; National Conference of Commissioners on Uniform State Laws, Uniform Health-Care Information Act, Minneapolis, MN, August 9, 1985. Some states include utilization review and similar activities in the exemption. See, e.g., Ariz. Rev. Stat. § 12-2294. Another common exemption from consent is disclosure of health information for purposes of obtaining payment. See, e.g., Fla. Stat. Ann. § 455.667; Tex. Rev. Civ. Stat. Art. 4495, § 5.08(h); 410 Ill. Comp. Stat. 50/3(d). Other common exemptions include disclosures for emergency care, and for disclosures to government authorities (such as a department of public health). See Gostin Study, at 1-2; 48-51. Some states also exempt disclosure to law enforcement officials (e.g., Massachusetts, Ch. 254 of the Acts of 2000), coroners (Wis. Stat. § 146.82), and for such purposes as business operations, oversight, research, and for directory information. Under these exceptions, providers can disclose health information without any consent or authorization from the patient. When states require specific, written authorization for disclosure of health information, the authorizations are usually only required for certain types of disclosures or certain types of information, and one authorization can suffice for multiple disclosures over time.

The states that do not have laws prohibiting disclosure of health information impose no specific requirements for consent or authorization prior to release of health information. There may, however, be other controls on release of health information. For instance, most health care professional licensure laws include general prohibitions against 'breaches of confidentiality.' In some states, patients can hold providers accountable for some unauthorized disclosures of health information about them under various tort theories, such as invasion of privacy and breach of a confidential relationship. While these controls may affect certain disclosure practices, they do not amount to a

requirement that a provider obtain authorization for each and every disclosure of health information.

Further, patients are typically not given a choice; they must sign the "consent" in order to receive care. As the Georgetown Study points out, "In effect, the authorization may function more as a waiver of consent -- the patient may not have an opportunity to object to any disclosures." Georgetown Study, Key Findings.

In the many cases where neither state law nor professional ethical standards exist, the only privacy protection individuals have is limited to the policies and procedures that the health care entity adopts. Corporate privacy policies are often proprietary. While several professional associations attached their privacy principles to their comments, health care entities did not. One study we found indicates that these policies are not adequate to provide appropriate privacy protections and alleviate public concern. The Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure made multiple findings highlighting the need for heightened privacy and security, including:

Finding 5: The greatest concerns regarding the privacy of health information derives from widespread sharing of patient information throughout the health care industry and the inadequate federal and state regulatory framework for systematic protection of health information.

For the Record: Protecting Electronic Health Information, National Academy Press, Washington DC, 1997.

Consent under this rule

In the NPRM, we expressed concern about the coercive nature of consents currently obtained by providers and plans relating to the use and disclosure of health information. We also expressed concern about the lack of information available to the patient during the process, and the fact that patients often were not even presented with a copy of the consent that they have signed. These and other concerns led us to propose that covered entities be permitted to use and disclose protected health information for treatment, payment and health care operations without the express consent of the subject individual.

In the final rule, we alter our proposed approach and require, in most instances, that health care providers who have a direct treatment relationship with their patients obtain the consent of their patients to use and disclose protected health information for treatment, payment and health care operations. While our concern about the coerced nature of these consents remains, many comments that we received from individuals, health care professionals, and organizations that represent them indicated that both patients and practitioners believe that patient consent is an important part of the current health care system and should be retained.

Providing and obtaining consent clearly has meaning for patients and practitioners. Patient advocates argued that the act of signing focuses the patient's attention on the substance of the transaction and provides an opportunity for the patient to ask questions about or seek modifications in the provider's practices. Many health care practitioners and their representatives argued that seeking a patient's consent to disclose confidential information is an ethical requirement that strengthens the physician-patient relationship. Both practitioners and patients argued that the approach proposed in the NPRM actually reduced patient protections by eliminating the opportunity for patients to agree to how their confidential information would be used and disclosed.

While we believe that the provisions in the NPRM that provided for detailed notice to the patient and the right to request restrictions would have provided an opportunity for patients and providers to discuss and negotiate over information practices, it is clear from the comments that many practitioners and patients believe the approach proposed in the NPRM is not an acceptable replacement for the patient providing consent. To encourage a more informed interaction between the patient and the provider during the consent process, the final rule requires that the consent form that is presented to the patient be accompanied by a notice that contains a detailed discussion of the provider's health information practices. The consent form must reference the notice and also must inform the patient that he or she has the right to ask the health care provider to request certain restrictions as to how the information of the patient will be used or disclosed. Our goal is to provide an opportunity for and to encourage more informed discussions between patients and providers about how protected health information will be used and disclosed within the health care system.

We considered and rejected other approaches to consent, including those that involved individuals providing a global consent to uses and disclosures when they sign up for insurance. While such approaches do require the patient to provide consent, it is not really an informed one or a voluntary one. It is also unclear how a consent obtained at the enrollment stage would be meaningfully communicated to the many providers who create the health information in the first instance. The ability to negotiate restrictions or otherwise have a meaningful discussion with the front-line provider would be independent of, and potentially in conflict with, the consent obtained at the enrollment stage. In addition, employers today are moving toward simplified enrollment forms, using check-off boxes and similar devices. The opportunity for any meaningful consideration or interaction at that point is slight. For these and other reasons, we decided that, to the extent a consent can accomplish the goal sought by individuals and providers, it must be focused on the direct interaction between an individual and provider.

The comments and fact-finding indicate that our approach will not significantly change the administrative aspect of consent as it exists today. Most direct treatment providers today obtain some type of consent for some uses and disclosures of health information. Our regulation will ensure that those consents cover the routine uses and disclosures of health information, and provide an opportunity for individuals to obtain further information and have further discussion, should they so desire.

Administrative Costs

Section 1172(b) of the Act provides that "[a]ny standard adopted under this part [part C of title XI of the Act] shall be consistent with the objective of reducing the administrative costs of providing and paying for health care." The privacy and security standards are the platform on which the remaining standards rest; indeed, the design of part C of title XI makes clear that the various standards are intended to function together. Thus, the costs of privacy and security are properly attributable to the suite of administrative simplification regulations as a whole, and the cost savings realized should likewise be calculated on an aggregated basis, as is done below. Because the privacy standards are an integral and necessary part of the suite of Administrative Simplification standards, and because that suite of standards will result in substantial administrative cost savings, the privacy standards are "consistent with the objective of reducing the administrative costs of providing and paying for health care."

As more fully discussed in the Regulatory Impact and Regulatory Flexibility analyses below, we recognize that these privacy standards will entail substantial initial and ongoing administrative costs for entities subject to the rules. It is also the case that the privacy standards, like the security standards authorized by section 1173(d) of the Act, are necessitated by the technological advances in information exchange that the remaining Administrative Simplification standards facilitate for the health care industry. The same technological advances that make possible enormous administrative cost savings for the industry as a whole have also made it possible to breach the security and privacy of health information on a scale that was previously inconceivable. The Congress recognized that adequate protection of the security and privacy of health information is a sine qua non of the increased efficiency of information exchange brought about by the electronic revolution, by enacting the security and privacy provisions of the law. Thus, as a matter of policy as well as law, the administrative standards should be viewed as a whole in determining whether they are "consistent with" the objective of reducing administrative costs.

Consultations

The Congress required the Secretary to consult with specified groups in developing the standards under sections 262 and 264. Section 264(d) of HIPAA specifically requires the Secretary to consult with the National Committee on Vital and Health Statistics (NCVHS) and the Attorney General in carrying out her responsibilities under the section. Section 1172(b)(3) of the Act, which was enacted by section 262, requires that, in developing a standard under section 1172 for which no standard setting organization has already developed a standard, the Secretary must, before adopting the standard, consult with the National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC), the Workgroup for Electronic Data Interchange (WEDI), and the American Dental Association (ADA). Section 1172(f) also requires the Secretary to rely on the recommendations of the NCVHS and consult with other appropriate federal and state agencies and private organizations.

We engaged in the required consultations including the Attorney General, NUBC, NUCC, WEDI and the ADA. We consulted with the NCVHS in developing the Recommendations, upon which this proposed rule is based. We continued to consult with this committee by requesting the committee to review the proposed rule and provide comments prior to its publication, and by reviewing transcripts of its public meeting on privacy and related topics. We consulted with representatives of the National Congress of American Indians, the National Indian Health Board, and the self governance tribes. We also met with representatives of the National Governors' Association, the National Conference of State Legislatures, the National Association of Public Health Statistics and Information Systems, and a number of other state organizations to discuss the framework for the proposed rule, issues of special interests to the states, and the process for providing comments on the proposed rule.

Many of these groups submitted comments to the proposed rule, and those were taken into account in developing the final regulation.

In addition to the required consultations, we met with numerous individuals, entities, and agencies regarding the regulation, with the goal of making these standards as compatible as possible with current business practices, while still enhancing privacy protection. During the open comment period, we met with dozens of groups.

Relevant federal agencies participated in the interagency working groups that developed the NPRM and the final regulation, with additional representatives from all operating divisions and many staff offices of HHS. The following federal agencies and offices were represented on the interagency working groups: the Department of Justice, the Department of Commerce, the Social Security Administration, the Department of Defense, the Department of Veterans Affairs, the Department of Labor, the Office of Personnel Management, and the Office of Management and Budget.

Go to Regulation Preamble, next section

Go to Regulation Text

Federal Register

Thursday,
February 20, 2003

Part II

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160, 162, and 164
Health Insurance Reform: Security Standards; Final Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160, 162, and 164

[CMS–0049–F]

RIN 0938–AI57

Health Insurance Reform: Security Standards

AGENCY: Centers for Medicare & Medicaid Services (CMS), HHS.

ACTION: Final rule.

SUMMARY: This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. The use of the security standards will improve the Medicare and Medicaid programs, and otherFederal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information. This final rule implements some of the requirements of the Administrative Simplification subtitle of the Health Insurance Portability andAccountability Act of 1996 (HIPAA).

DATES: *Effective Date:* These regulations are effective on April 21, 2003.

Compliance Date: Covered entities, with the exception of small health plans, must comply with the requirements of this final rule by April 21, 2005. Small health plans must comply with the requirements of this final rule by April 21, 2006.

FOR FURTHER INFORMATION CONTACT: William Schooler, (410) 786–0089.

SUPPLEMENTARY INFORMATION:

Availability of Copies and Electronic Access

To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512–1800 or by faxing to (202) 512–2250. The cost for each copy is $10. As an alternative, you can view and photocopy the **Federal Register** document at most libraries designated as Federal Depository Libraries and at many other public and academic libraries throughout the country that receive the **Federal Register**.

This **Federal Register** document is also available from the **Federal Register** online database through GPO access, a service of the U.S. Government Printing Office. The Web site address is *http://www.access.gpo.gov/nara/index.html*.

I. Background

The Department of Health and Human Services (HHS) Medicare Program, other Federal agencies operating health plans or providing health care, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Currently, no standard measures exist in the health care industry that address all aspects of the security of electronic health information while it is being stored or during the exchange of that information between entities.

This final rule adopts standards as required under title II, subtitle F, sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191. These standards require measures to be taken to secure this information while in the custody of entities covered by HIPAA (covered entities) as well as in transit between covered entities and from covered entities to others.

The Congress included provisions to address the need for safeguarding electronic health information and other administrative simplification issues in HIPAA. In subtitle F of title II of that law, the Congress added to title XI of the Social Security Act a new part C, entitled ''Administrative Simplification'' (hereafter, we refer to the Social Security Act as ''the Act''; we refer to the other laws cited in this document by their names). The purpose of subtitle F is to improve the Medicare program under title XVIII of the Act, the Medicaid program under title XIX of the Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements to enable the electronic exchange of certain health information.

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose requirements on HHS, health plans, health care clearinghouses, and certain health care providers. These statutory sections are discussed in the Transactions Rule, at 65 FR 50312, on pages 50312 through 50313, and in the final rules adopting Standards for Privacy of Individually Identifiable Health Information, published on December 28, 2000 at 65 FR 82462 (Privacy Rules), on pages 82470 through 82471, and on August 14, 2002 at 67 FR 53182. The reader is referred to those discussions.

Section 1173(d) of the Act requires the Secretary of HHS to adopt security standards that take into account the technical capabilities of record systems used to maintain health information, the costs of security measures, the need to train persons who have access to health information, the value of audit trails in computerized record systems, and the needs and capabilities of small health care providers and rural health care providers. Section 1173(d) of the Act also requires that the standards ensure that a health care clearinghouse, if part of a larger organization, has policies and security procedures that isolate the activities of the clearinghouse with respect to processing information so as to prevent unauthorized access to health information by the larger organization. Section 1173(d) of the Act provides that covered entities that maintain or transmit health information are required to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information and to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information. These safeguards must also otherwise ensure compliance with the statute by the officers and employees of the covered entities.

II. General Overview of the Provisions of the Proposed Rule

On August 12, 1998, we published a proposed rule (63 FR 43242) to establish a minimum standard for security of electronic health information. We proposed that the standard would require the safeguarding of all electronic health information by covered entities. The proposed rule also proposed a

standard for electronic signatures. This final rule adopts only security standards. All comments concerning the proposed electronic signature standard, responses to these comments, and a final rule for electronic signatures will be published at a later date. A detailed discussion of the provisions of the August 12, 1998 proposed rule can be found at 63 FR 43245 through 43259.

We originally proposed to add part 142, entitled ''Administrative Requirements,'' to title 45 of the Code of Federal Regulations (CFR). It has now been determined that this material will reside in subchapter C of title 45, consisting of parts 160, 162, and 164. Subpart A of part 160 contains the general provisions applicable to all the Administrative Simplification rules; other subparts of part 160 will contain other requirements applicable to all standards. Part 162 contains the standards for transactions and code sets and will contain the identifier standards. Part 164 contains the standards relating to privacy and security. Subpart A of part 164 contains general provisions applicable to part 164; subpart E contains the privacy standards. Subpart C of part 164, which is adopted in this final rule, adopts standards for the security of electronic protected health information.

III. Analysis of, and Responses to, Public Comments on the Proposed Rule

We received approximately 2,350 timely public comments on the August 12, 1998 proposed rule. The comments came from professional associations and societies, health care workers, law firms, health insurers, hospitals, and private individuals. We reviewed each commenter's letter and grouped related comments. Some comments were identical. After associating like comments, we placed them in categories based on subject matter or based on the section(s) of the regulations affected and then reviewed the comments.

In this section of the preamble, we summarize the provisions of the proposed regulations, summarize the related provisions in this final rule, and respond to comments received concerning each area.

It should be noted that the proposed Security Rule contained multiple proposed ''requirements'' and ''implementation features.'' In this final rule, we replace the term ''requirement'' with ''standard.'' We also replace the phrase ''implementation feature'' with ''implementation specification.'' We do this to maintain consistency with the use of those terms as they appear in the statute, the Transactions Rule, and the Privacy Rule. Within the comment and response portion of this final rule, for purposes of continuity, however, we use ''requirement'' and ''implementation feature'' when we are referring specifically to matters from the proposed rule. In all other instances, we use ''standard'' and ''implementation specification.''

The proposed rule would require that each covered entity (as now described in § 160.102) engaged in the electronic maintenance or transmission of health information pertaining to individuals assess potential risks and vulnerabilities to such information in its possession in electronic form, and develop, implement, and maintain appropriate security measures to protect that information. Importantly, these measures would be required to be documented and kept current.

The proposed security standard was based on three basic concepts that were derived from the Administrative Simplification provisions of HIPAA. First, the standard should be comprehensive and coordinated to address all aspects of security. Second, it should be scalable, so that it can be effectively implemented by covered entities of all types and sizes. Third, it should not be linked to specific technologies, allowing covered entities to make use of future technology advancements.

The proposed standard consisted of four categories of requirements that a covered entity would have to address in order to safeguard the integrity, confidentiality, and availability of its electronic health information pertaining to individuals: administrative procedures, physical safeguards, technical security services, and technical mechanisms. The implementation features described the requirements in greater detail when that detail was needed. Within the four categories, the requirements and implementation features were presented in alphabetical order to convey that no one item was considered to be more important than another.

The four proposed categories of requirements and implementation features were depicted in tabular form along with the electronic signature standard in a combined matrix located at Addendum 1. We also provided a glossary of terms, at Addendum 2, to facilitate a common understanding of the matrix entries, and at Addendum 3, we mapped available existing industry standards and guidelines to the proposed security requirements.

A. General Issues

The comment process overwhelmingly validated our basic assumptions that the entities affected by this regulation are so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be useable by all covered entities. Many commenters also supported the concept of technological neutrality, which would afford them the flexibility to select appropriate technology solutions and to adopt new technology over time.

1. Security Rule and Privacy Rule Distinctions

As many commenters recognized, security and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information. It is important that we note several distinct differences between the Privacy Rule and the Security Rule.

The security standards below define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The standards require covered entities to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission. The Privacy Rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information.

As is discussed more fully below, this rule narrows the scope of the information to which the safeguards must be applied from that proposed in the proposed rule, electronic health information pertaining to individuals, to protected health information in electronic form. Thus, the scope of information covered in this rule is consistent with the Privacy Rule, which addresses privacy protections for ''protected health information.'' However, the scope of the Security Rule is more limited than that of the Privacy Rule. The Privacy Rule applies to protected health information in any form, whereas this rule applies only to protected health information in electronic form. It is true that, under section 1173(d) of the Act, the Secretary has authority to cover ''health information,'' which, by statute, includes information in other than electronic form. However, because the proposed rule proposed to cover only health information in electronic form, we do not include security standards for health information in non-electronic form in this final rule.

We received a number of comments that pertained to privacy issues. These issues were considered in the development of the Privacy Rule and many of these comments were addressed in the preamble of the Privacy Rule. Therefore, we are referring the reader to that document for a discussion of those issues.

2. Level of Detail

We solicited comments as to the level of detail expressed in the required implementation features; that is, we specifically wanted to know whether commenters believe the level of detail of any proposed requirement went beyond what is necessary or appropriate. We received numerous comments expressing the view that the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress. We have accordingly written the final rule to frame the standards in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies.

3. Implementation Specifications

In addition to adopting standards, this rule adopts implementation specifications that provide instructions for implementing those standards.

However, in some cases, the standard itself includes all the necessary instructions for implementation. In these instances, there may be no corresponding implementation specification for the standard specifically set forth in the regulations text. In those instances, the standards themselves also serve as the implementation specification. In other words, in those instances, we are adopting one set of instructions as both the standard and the implementation specification. The implementation specification would, accordingly, in those instances be required.

In this final rule, we adopt both ''required'' and ''addressable'' implementation specifications. We introduce the concept of ''addressable implementation specifications'' to provide covered entities additional flexibility with respect to compliance with the security standards.

In meeting standards that contain addressable implementation specifications, a covered entity will ultimately do one of the following: (a) Implement one or more of the addressable implementation specifications; (b) implement one or more alternative security measures; (c) implement a combination of both; or (d) not implement either an addressable implementation specification or an alternative security measure. In all cases, the covered entity must meet the standards, as explained below.

The entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. Based upon this decision the following applies:

(a) If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must implement it.

(b) If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an additional security safeguard, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification. An entity that meets a given standard through alternative measures must document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard. For example, the addressable implementation specification for the integrity standard calls for electronic mechanisms to corroborate that data have not been altered or destroyed in an unauthorized manner (see 45 CFR 164.312(c)(2)). In a small provider's office environment, it might well be unreasonable and inappropriate to make electronic copies of the data in question. Rather, it might well be more practical and afford a sufficient safeguard to make paper copies of the data.

(c) A covered entity may also decide that a given implementation specification is simply not applicable (that is, neither reasonable nor appropriate) to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met. For example, under the information access management standard, an access establishment and modification implementation specification reads: ''implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process'' (45 CFR 164.308(a)(4)(ii)(c)). It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals.

a. *Comment:* A large number of commenters indicated that mandating 69 implementation features would result in a regulation that is too burdensome, intrusive, and difficult to implement. These commenters requested that the implementation features be made optional to meet the requirements. A number of other commenters requested that all implementation features be removed from the regulation.

Response: Deleting the implementation specifications would result in the standards being too general to understand, apply effectively, and enforce consistently. Moreover, a number of implementation specifications are so basic that no covered entity could effectively protect electronic protected health information without implementing them. We selected 13 of these mandatory implementation specifications based on (1) the expertise of Federal security experts and generally accepted industry practices and, (2) the recommendation for immediate implementation of certain technical and organizational practices and procedures described in Chapter 6 of *For The Record: Protecting Electronic Health Information,* a 1997 report by the National Research Council (NRC). These mandatory implementation specifications are referred to as required implementation specifications and are reflected in the NRC report's recommendations. Risk Analysis and Risk management are found in the NRC recommendation title System Assessment; Sanction Policy is required in the Sanctions recommendation; Information system Activity Review is discussed in Audit Trails; Response and Reporting circumstances.

In addition, a number of voluntary national and regional organizations have been formed to address HIPAA implementation issues and to facilitate

communication among trading partners. These include the Strategic National Implementation Process (SNIP) developed under the auspices of the Workgroup for Electronic Data Interchange (WEDI), an organization named in the HIPAA statute to consult with the Secretary of HHS on HIPAA issues. Some of these organizations have developed white papers, tools, and recommended best practices addressing a number of HIPAA issues, including security. Covered entities may wish to examine these products to determine if they are relevant and useful in their own implementation efforts. A partial list of these organizations can be found at *http://www.wedi/snip./org.* We believe that these and other future industry-developed guidelines and/or models may provide valuable assistance to covered entities implementing these standards but must caution that HHS does not rate or endorse any such guidelines and/or models and the value of its content must be determine by the user.

b. *Comment:* Many commenters asked us to develop guidelines and models to aid in complying with the Security Rule. Several commenters either offered to participate in the development of guidelines and models or suggested entities that should be invited to participate.

Response: We agree that creation of compliance tools and guidelines for different business environments could assist covered entities to implement the HIPAA Security Rule. We plan to issue guidance documents after the publication of this final rule. However, it is critical for each covered entity to establish policies and procedures that address its own unique risks and circumstances.

In addition, a number of voluntary national and regional organizations have been formed to address HIPAA implementation issues and to facilitate communication among trading partners. These include the Strategic National Implementation Process (SNIP) developed under the auspices of the Workgroup for Electronic Data Interchange (WEDI), an organization named in the HIPAA statute to consult with the Secretary of HHS on HIPAA issues. Some of these organizations have developed white papers, tools, and recommended best practices addressing a number of HIPAA issues, including security.

Covered entities may wish to examine these products to determine if they are relevant and useful in their own implementation efforts. A partial list of these organizations can be found at *http://www.snip.wedi.org.* We believe that these and other future industry-developed guidelines and/or models may provide valuable assistance to covered entities implementing these standards but must caution that HHS does not rate or endorse any such guidelines and/or models and the value of its content must be determined by the user.

4. Examples

Comment: We received a number of comments that demonstrated confusion regarding the purpose of the examples of security solutions that were included throughout the proposed rule. Commenters stated that they could not, or did not wish to, adopt various security measures suggested in examples. Other commenters asked that we include additional options within the examples. Some commenters referred specifically to the example provided in the proposed rule demonstrating how a small or rural provider might comply with the standards. One commenter asked for clarification that the examples are not mandatory measures that are required to demonstrate compliance, but are merely meant as a guide when implementing the security standards. Another commenter expressed support for the use of examples to clarify the intent of text descriptions.

Response: We wish to clarify that examples are used only as illustrations of possible approaches, and are included to serve as a springboard for ideas. The steps that a covered entity will actually need to take to comply with these regulations will be dependent upon its own particular environment and circumstances and risk assessment. The examples do not describe mandatory measures, nor do they represent the only, or even the best, way of achieving compliance. The most appropriate means of compliance for any covered entity can only be determined by that entity assessing its own risks and deciding upon the measures that would best mitigate those risks.

B. Applicability (§ 164.302)

We proposed that the security standards would apply to health plans, health care clearinghouses, and to health care providers that maintain or transmit health information electronically. The proposed security standards would apply to all electronic health information maintained or transmitted, regardless of format (standard transaction or a proprietary format). No distinction would be made between internal corporate entity communication or communication external to the corporate entity. Electronic transmissions would include transactions using all media, even when the information is physically moved from one location to another using magnetic tape, disk, or other machine readable media. Transmissions over the Internet (wide-open), extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks would be included. We proposed that telephone voice response and ''faxback'' systems (a request for information made via voice using a fax machine and requested information returned via that same machine as a fax) would not be included but we solicited comments on this proposed exclusion.

This final rule simplifies the applicability statement greatly. Section 164.302 provides that the security standards apply to covered entities; the scope of the information covered is specified in § 164.306 (see the discussion under that section below regarding the changes and revisions to the scope of information covered).

1. *Comment:* A number of commenters requested clarification of who must comply with the standards. The preamble and proposed § 142.102 and § 142.302 stated: ''Each person described in section 1172(a) of the Act who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards.'' Commenters suggested that this statement is in conflict with the law, which defines a covered entity as a health plan, a clearinghouse, or a health care provider that conducts certain transactions electronically. The commentors apparently did not realize that section 1172(a) of the Act contains the definition of covered entities.

Response: Section 164.302 below makes the security standards applicable to ''covered entities.'' The term ''covered entity'' is defined at § 160.103 as one of the following: (1) A health plan; (2) a health care clearinghouse; (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by part 162 of title 45 of the Code of Federal Regulations (CFR). The rationale for the use and the meaning of the term ''covered entity'' is discussed in the preamble to the Privacy Rule (65 FR 82476 through 82477).

As that discussion makes clear, the standards only apply to health care providers who engage electronically in the transactions for which standards have been adopted.

2. *Comment:* Several commenters recommended expansion of applicability, either to other specific entities, or to all entities involved in health care. Others wanted to know whether the standards apply to entities such as employers, public health organizations, medical schools, universities, research organizations, plan brokers, or non-EDI providers. One commenter asked whether the standards apply to State data organizations operating in capacities other than as plans, clearinghouses, or providers. Still other commenters stated that it was inappropriate to include physicians and other health care professionals in the same category as plans and clearinghouses, arguing that providers should be subject to different, less burdensome requirements because they already protect health information.

Response: The statute does not cover all health care entities that transmit or maintain individually identifiable health information. Section 1172(a) of the Act provides that only health plans, health care clearinghouses, and certain health care providers (as discussed above) are covered. With respect to the comments regarding the difference between providers and plans/clearinghouses, we have structured the Security Rule to be scalable and flexible enough to allow different entities to implement the standards in a manner that is appropriate for their circumstances. Regarding the coverage of entities not within the jurisdiction of HIPAA, *see* the Privacy Rule at 82567 through 82571.

3. *Comment:* One commenter asked whether the standards would apply to research organizations, both to those affiliated with health care providers and those that are not.

Response: Only health plans, health care clearinghouses, and certain health care providers are required to comply with the security standards. Researchers who are members of a covered entity's work force may be covered by the security standards as part of the covered entity. *See* the definition of ''workforce'' at 45 CFR 160.103. Note, however, that a covered entity could, under appropriate circumstances, exclude a researcher or research division from its health care component or components (*see* § 164.105(a)). Researchers who are not part of the covered entity's workforce and are not themselves covered entities are not subject to the standards.

4. *Comment:* Several commenters stated that internal networks and external networks should be treated differently. One commenter asked for further clarification of the difference between what needs to be secured external to a corporation versus the security of data movement within an organization. Another stated that complying with the security standards for internal communications may prove difficult and costly to monitor and control. In contrast, one commenter stated that the existence of requirements should not depend on whether use of information is for internal or external purposes.

Another commenter argued that the regulation goes beyond the intent of the law, and while communication of electronic information between entities should be covered, the law was never intended to mandate changes to an entity's internal automated systems. One commenter requested that raw data that are only for the internal use of a facility be excluded, provided that reasonable safeguards are in place to keep the raw data under the control of the facility.

Response: Section 1173(d)(2) of the Act states: Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—(A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated—(i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person.

This language draws no distinction between internal and external data movement. Therefore, this final rule covers electronic protected health information at rest (that is, in storage) as well as during transmission. Appropriate protections must be applied, regardless of whether the data are at rest or being transmitted. However, because each entity's security needs are unique, the specific protections determined appropriate to adequately protect information will vary and will be determined by each entity in complying with the standards (*see* the discussion below).

5. *Comment:* Several commenters found the following statement in the proposed rule (63 FR 43245) at section II.A. confusing and asked for clarification: ''With the exception of the security standard, transmission within a corporate entity would not be required to comply with the standards.''

Response: In the final Transactions Rule, we revised our approach concerning the transaction and code set exemptions, replacing this concept with other tests that determine whether a particular transaction is subject to those standards (*see* the discussion in the Transactions Rule at 65 FR 50316 through 50318). We also note that the Privacy Rule regulates a covered entity's use, as well as disclosure, of protected health information.

6. *Comment:* One commenter stated that research would be hampered if proposed § 142.306(a) applied. The commenter believes that research uses of health information should be excluded or the standard should be revised to allow appropriate flexibility for research depending on the risk to patients or subjects (for example, if the information is anonymous, there is no risk, and it would not be necessary to meet the security standards).

Response: If electronic protected health information is de-identified (as truly anonymous information would be), it is not covered by this rule because it is no longer electronic protected health information (see 45 CFR 164.502(d) and 164.514(a)). Electronic protected health information received, created, or maintained by a covered entity, or that is transmitted by covered entities, is covered by the security standards and must be protected. To the extent a researcher is a covered entity, the researcher must comply with these standards with respect to electronic protected health information. Otherwise, the conditions for release of such information to researchers is governed by the Privacy Rule. *See,* for example, 45 CFR 164.512(i), 164.514(e) and 164.502(d). These standards would not apply to the researchers as such in the latter circumstances.

7. *Comment:* One commenter asked to what extent individual patients are subject to the standards. For example, some telemedicine practices support the use of diagnostic systems in the patient's home, which can be used to conduct tests and send results to a remote physician. In other cases, patients may be responsible for the filing of insurance claims directly and will need the ability to verify facts, confirm receipt of claims, and so on. The commenter asked if it is the intent of the rule to include electronic transmission to or from the patient.

Response: Patients are not covered entities and, thus, are not subject to these standards. With respect to transmissions from covered entities, covered entities must protect electronic protected health information when they transmit that information. *See* also the discussion of encryption in section III.G.

C. Transition to the Final Rule

The proposed rule included definitions for a number of terms that have now already been promulgated as part of the Transactions Rule or the Privacy Rule. Comments related to the definitions of ''code set,'' ''health care'' clearinghouse,'' ''health plan,'' ''health care provider,'' ''small health plan,'' ''standard'' and ''transaction,'' are addressed in the Transactions Rule at 65 FR 50319 through 50320. Comments concerning the definition of ''individually identifiable health information'' are discussed below, but are also addressed in the Privacy Rule at 65 FR 82611 through 82613. In addition, a few terms were redefined in the final Standards for Privacy of Individually Identifiable Health Information (67 FR 53182), issued on August 14, 2002 (Privacy Modifications). Certain terms that were defined in the proposed rule are not used in the final rule because they are no longer necessary. Other terms defined in the proposed rule are defined within the explanation of the standards in the final rule and are discussed in the preamble discussions in § 164.308 through § 164.312.

Definitions of terms relevant to the security standards now appear in the regulations text provisions as indicated below:

§ 160.103: Definitions of the following terms relevant to this rule appear in § 160.103: ''business associate,'' ''covered entity,'' ''disclosure,'' ''electronic media,'' ''electronic protected health information,'' ''health care,'' ''health care clearinghouse,'' ''health care provider,'' ''health information,'' ''health plan,'' ''individual,'' ''individually identifiable health information,'' ''implementation specification,'' ''organized health care arrangement,'' ''protected health information,'' ''standard,'' ''use,'' and ''workforce.'' These terms were discussed in connection with the Transaction and Privacy Rules and with the exception of the terms ''covered entity'' ''disclosure'' ''electronic protected health information,'' ''health information,'' ''individual,'' ''organized health care arrangement,'' ''protected health information,'' and ''use,'' we will not discuss them in this document. We note that the definition of those terms are not changed in the final rule.

§ 162.103: We have moved the definition of ''electronic media'' at § 162.103 to § 160.103 and have modified it to clarify that the term includes storage of information. The term ''electronic media'' is used in the definition of ''protected health information.'' Both the privacy and security standards apply to information ''at rest'' as well as to information being transmitted.

We note that we have deleted the reference to § 162.103 in paragraph (1)(ii) of the definition of ''protected health information,'' since both definitions, ''electronic media'' and ''protected health information,'' have been moved to this section. Also, it is unnecessary, because the definitions of § 160.103 apply to all of the rule in parts 160, 162, and 164.

We have also clarified that the physical movement of electronic media from place to place is not limited to magnetic tape, disk, or compact disk. This clarification removes a restriction as to what is considered to be physical electronic media, thereby allowing for future technological innovation. We further clarified that transmission of information not in electronic form before the transmission, for example, paper or voice, is not covered by this definition.

§ 164.103: The following term ''plan sponsor'' now appears in the new § 164.103, which consists of definitions of terms common to both subpart C and subpart E (the privacy standards). This definition was moved, without substantive change, from § 164.501 and has the meaning given to it in that section, and comments relating to this definition are discussed in connection with that section in the Privacy Rule at 65 FR 82607, 82611 through 82613, 82618 through 82622, and 82629.

§ 164.304: Definitions specifically applicable to the Security Rule appear in § 164.304, and these are discussed below. These definitions are from, or derived from, currently accepted definitions in industry publications, such as, the International Organization for Standards (ISO) 7498–2 and the American Society for Testing and Materials (ASTM) E1762–95.

The following terms in § 164.304 are taken from the proposed rule text or the glossary in Addendum 2 of the proposed rule (63 FR 43271), were not commented on, and/or are unchanged or have only minor technical changes for purposes of clarification and are not discussed below: ''access,'' ''authentication,'' ''availability,'' ''confidentiality,'' ''encryption,'' ''password,'' and ''security.''

§ 164.314: Four terms were defined in § 164.504(a) of the Privacy Rule (''common control,'' ''common ownership,'' ''health care component,'' and ''hybrid entity''). Because these terms apply to both security and privacy, their definitions have been moved to § 164.103 without change. Those terms are discussed in the Privacy Rule at 65 FR 82502 through 82503 and at 67 FR 53203 through 53207.

1. Covered Entity (§ 160.103)

Comment: One commenter asked if transcription services were covered entities. The question arose because transcription is often the first electronic or printed source of clinical information. Concern was expressed about the application of physical safeguard standards to the transcribers working for transcription companies or health care providers, either as employees or as independent contractors.

Another commenter expressed concern that scalability was limited to only small providers. The commenter explained that Third Party Administrators (TPAs) allow claim processors to work at home. Some TPAs have noted that it would be impossible to comply with the security standards for home-based claims processors.

Response: A covered entity's responsibility to implement security standards extends to the members of its workforce, whether they work at home or on-site. Because a covered entity is responsible for ensuring the security of the information in its care, the covered entity must include ''at home'' functions in its security process. While an independent transcription company or a TPA may not be covered entities, they will be a business associate of the covered entity because their activities fall under paragraph (1)(i)(a) of the definition of that term. For business associate provisions see proposed preamble section III.E.8. and § 164.308(b)(1) and § 164.314(c) of this final rule.

2. Health Care and Medical Care (§ 160.103)

Comment: One commenter asked whether ''medical care,'' which is defined in the proposed rule, and ''health care,'' which is not, are synonymous.

Response: The term ''medical care,'' as used in the proposed rule (63 FR 43242), was intended to be synonymous with ''health care.'' The term ldquo;medical care'' is not included in this final rule. It is, however, included in the definition of ''health plan,'' where its meaning is not synonymous with ''health care.'' For a full discussion of this issue and its resolution, *see* the Privacy Rule (65 FR 82578).

3. Health Information and Individually Identifiable Health Information 160.103)

We note that the definitions of ''health information'' and ''individually identifiable health information'' remain unchanged from those published in the Transactions and Privacy Rules.

a. *Comment:* A number of commenters asked that the definition of ''health information'' be expanded to include information collected by additional entities. Several commenters wanted the definition to include health information collected, maintained, or transmitted by any entity, and one commenter suggested the inclusion of aggregated information not identifiable to an individual. Several commenters asked that eligibility information be excluded from the definition of information. Several commenters wanted the definition broadened to include demographics.

Response: Our definition of health information is taken from the definition in section 1171(4) of the Act, which provides that health information relates to the health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual. The statutory definition also specifies the entities by which health information is created or received. We note that, because ''individually identifiable health information'' is a subset of ''health information'' and by statute includes demographic information, ''health information'' necessarily includes demographic information. We think this is clear as a matter of statutory construction and does not require further regulatory change.

b. *Comment:* Several commenters asked that we clarify the difference between ''health information'' and ''individually identifiable'' and ''health information pertaining to an individual'' as used in the August 12, 1998 proposed rule (63 FR 43242). Additionally, commenters asked that we be more consistent in the use of these terms and recommended use of the term ''individually identifiable health information.''

Two commenters stated that it is important to distinguish between ''health information pertaining to an individual'' and ''individually identifiable health information,'' as in reporting statistics at various levels there will always be a need to bring forth information pertaining to an individual.

One commenter recommended that the standards apply only to individually identifiable health information. Another stated that in § 142.306(b) of the proposed rule, ''health information pertaining to an individual'' should be changed to ''individually identifiable health information,'' as nonidentifiable information can be used for utilization review and other purposes. As written, the regulation text could limit the ability to use data, for example, from a clearinghouse for compliance monitoring.

Response: In general, we agree with these commenters, and note that these comments are largely mooted by the decision, reflected in § 164.306 below and discussed in section III.D.1. of this final rule, to cover only electronic protected health information in this final rule.

c. *Comment:* Several commenters stated that the definition of ''individually identifiable health information'' is not in the regulations and should be added.

Response: We note that the definition of ''individually identifiable health information'' appears at § 160.103, which applies to this final rule.

4. Protected Health Information (§ 160.103)

This term is moved from § 164.501 to § 160.103 because it applies to both subparts C (security) and E (privacy). See 67 FR 53192 through 531936 regarding the definition of ''protected health information.''

Also, the term ''electronic media'' is included in paragraphs (1)(i) and (ii) of the definition of ''protected health information,'' as specified in this section.

In addition, we added the definitions of ''covered functions,'' ''plan sponsor,'' and ''Required by law'' to § 164.103.

5. Breach (§ 164.304)

Comment: One commenter asked that ''breach'' be defined.

Response: The term ''breach'' has been deleted and therefore not defined. Instead, we define the term ''security incident,'' which better describes the types of situations we were referring to as breaches.

6. Facility (§ 164.304)

This new term has been added as a result of changing the name of the ''physical access control'' standard to ''facility access control.'' This change was made based on comments indicating that the original term was not descriptive. We have defined the term ''facility'' as the physical premises and interior and exterior of a building.

7. Security Incident (§ 164.304)

Comment: We received comments asking that this term be defined.

Response: This final rule defines ''Security incident'' in § 164.304 as ''the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.''

8. System (§ 164.304)

Comment: One commenter asked that ''system'' be defined.

Response: This final rule defines ''system,'' in the context of an information system, in § 164.304 as ''an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.''

9. Workstation (§ 164.304)

Comment: One commenter expressed concern that the use of the term ''workstation'' implied limited applicability to fixed devices (such as terminals), excluding laptops and other portable devices.

Response: We have added a definition of the term ''workstation'' to clarify that portable devices are also included. This final rule defines workstation as ''an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.''

10. Definitions Not Adopted

Several definitions in the proposed regulations text and glossary are not adopted as definitions in the final rule: ''participant,'' ''contingency plan,'' ''risk,'' ''role-based access control,'' and ''user-based access control.'' The terms ''participant,'' ''role-based access control,'' and ''user-based access control'' are not used in this final rule and thus are not defined. ''Risk'' is not defined as its meaning is generally understood. While we do not define the term, we address ''contingency plan'' as a standard in § 164.308(a)(7) below.

a. *Comment:* We received comments requesting that we define the following terms: ''token'' and ''documentation.''

Response: These terms were defined in Addendum 2 of the proposed rule. In this final rule, we do not adopt a definition for ''token'' because it is not used in the final rule. ''Documentation'' is discussed in § 164.316 below.

b. *Comment:* We received several comments that ''small'' and ''rural'' should be defined as those terms apply

to providers. We received an equal number of comments stating that there is no need to define these terms. One commenter stated that definitions for these terms would be necessary only if special exemptions existed for small and rural providers. Several commenters suggested initiation of a study to determine limitations and potential barriers small and rural providers will have in implementing these regulations.

Response: The statute requires that we address the needs of small and rural providers. We believe that we have done this through the provisions, which require the risk assessment and the response to be assessment based on the needs and capabilities of the entity. This scalability concept takes the needs of those providers into account and eliminates any need to define those terms.

c. *Comment:* In the proposed rule, we proposed the following definition for the term ''Access control'': ''A method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation.'' One commenter believed the proposed definition is too restrictive and requested revision of the definition to read: ''Access control refers to a method of restricting access to resources, allowing access to only those entities which have been specifically granted the desired access rights.'' Another commenter wanted the definition expanded to include partitioned rule-based access control (PRBAC).

Response: We agree with the commenter who suggested that the definition as proposed seemed too restrictive. In this case, as in many others, a number of commenters believed the examples given in the proposed rule provided the only acceptable compliance actions. As previously noted, in order to clarify that the examples listed were not to be considered all-inclusive, we have generalized the proposed requirements in this final rule. In this case, we have also generalized the requirements and placed the substantive provisions governing access control at § 164.308(a)(4), § 164.310(a)(1), and § 164.312(a)(1). With respect to PRBAC, the access control standard does not exclude this control, and entities should adopt it if appropriate to their circumstances.

D. General Rules (§ 164.306)

In the proposed rule, we proposed to cover all health information maintained or transmitted in electronic form by a covered entity. We proposed to adopt, in § 142.308, a nation-wide security standard that would require covered entities to implement security measures that would be technology-neutral and scalable, and yet integrate all the components of security (administrative procedures, physical safeguards, technical security services, and technical security mechanisms) that must be in place to preserve health information confidentiality, integrity, and availability (three basic elements of security). Since no comprehensive, scalable, and technology-neutral set of standards currently exists, we proposed to designate a new standard, which would define the security requirements to be fulfilled.

The proposed rule proposed to define the security standard as a set of scalable, technology-neutral requirements with implementation features that providers, plans, and clearinghouses would have to include in their operations to ensure that health information pertaining to an individual that is electronically maintained or electronically transmitted remains safeguarded. The proposed rule would have required that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its own unique security needs. How individual security requirements would be satisfied and which technology to use would be business decisions that each entity would have to make.

In the final rule we adopt this basic framework. In § 164.306, we set forth general rules pertaining to the security standards. In paragraph (a), we describe the general requirements. Paragraph (a) generally reflects section 1173(d)(2) of the Act, but makes explicit the connection between the security standards and the privacy standards (see § 164.306(a)(3)). In § 164.306(a)(1), we provide that the security standards apply to all electronic protected health information the covered entity creates, receives, maintains, or transmits. In paragraph (b)(1), we provide explicitly for the scalability of this rule by discussing the flexibility of the standards, and paragraph (b)(2) of § 164.306 discusses various factors covered entities must consider in complying with the standards.

The provisions of § 164.306(c) provide the framework for the security standards, and establish the requirement that covered entities must comply with the standards. The administrative, physical, and technical safeguards a covered entity employs must be reasonable and appropriate to accomplish the tasks outlined in paragraphs (1) through (4) of § 164.306(a). Thus, an entity's risk analysis and risk management measures required by § 164.308(a)(1) must be designed to lead to the implementation of security measures that will comply with § 164.306(a).

It should be noted that the implementation of reasonable and appropriate security measures also supports compliance with the privacy standards, just as the lack of adequate security can increase the risk of violation of the privacy standards. If, for example, a particular safeguard is inadequate because it routinely permits reasonably anticipated uses or disclosures of electronic protected health information that are not permitted by the Privacy Rule, and that could have been prevented by implementation of one or more security measures appropriate to the scale of the covered entity, the covered entity would not only be violating the Privacy Rule, but would also not be in compliance with § 164.306(a)(3) of this rule.

Paragraph (d) of § 164.306 establishes two types of implementation specifications, required and addressable. It provides that required implementation specifications must be met. However, with respect to implementation specifications that are addressable, § 164.306(d)(3) specifies that covered entities must assess whether an implementation specification is a reasonable and appropriate safeguard in its environment, which may include consideration of factors such as the size and capability of the organization as well as the risk. If the organization determines it is a reasonable and appropriate safeguard, it must implement the specification. If an addressable implementation specification is determined not to be a reasonable and appropriate answer to a covered entity's security needs, the covered entity must do one of two things: implement another equivalent measure if reasonable and appropriate; or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure at all. The covered entity must document the rationale behind not implementing the implementation specification. See the detailed discussion in section II.A.3.

Paragraph (e) of § 164.306 addresses the requirement for covered entities to maintain the security measures

implemented by reviewing and modifying the measures as needed to continue the provision of reasonable and appropriate protections, for example, as technology moves forward, and as new threats or vulnerabilities are discovered.

1. Scope of Health Information Covered by the Rule (§ 164.306(a))

We proposed to cover health information maintained or transmitted by a covered entity in electronic form. We have modified, by narrowing, the scope of health information to be safeguarded under this rule from that which was proposed. The statute requires the privacy standards to cover individually identifiable health information. The Privacy Rule covers all individually identifiable information except for: (1) Education records covered by the Family and Educational Rights and Privacy Act (FERPA); (2) records described in 20 U.S.C. 1232g(a)(4)(B)(iv); and (3) employment records. (see the Privacy Rule at 65 FR 82496. See also 67 FR 53191 through 53193). The scope of information covered in the Privacy Rule is referred to as ''protected health information.'' Based upon the comments we received, we align the requirements of the Security and Privacy Rules with regard to the scope of information covered, in order to eliminate confusion and ease implementation. Thus, this final rule requires protection of the same scope of information as that covered by the Privacy Rule, except that it only covers that information if it is in electronic form.

We note that standards for the security of all health information or protected health information in nonelectronic form may be proposed at a later date.

a. *Comment:* One commenter stated that the rule should apply to aggregate information that is not identifiable to an individual. In contrast, another commenter asked that health information used for statistical analysis be exempted if the covered entity may reasonably expect that the removed information cannot be used to re-identify an individual.

Response: As a general proposition, any electronic protected health information received, created, maintained, or transmitted by a covered entity is covered by this final rule. We agree with the second commenter that certain information, from which identifiers have been stripped, does not come within the purview of this final rule. Information that is de-identified, as defined in the Privacy Rule at § 164.502(d) and § 164.514(a), is not ''individually identifiable'' within the meaning of these rules and, thus, does not come within the definition of ''protected health information.'' It accordingly is not covered by this final rule. For a full discussion of the issues of de-identification and re-identification of individually identifiable health information see 65 FR 82499 and 82708 through 82712 and 67 FR 53232 through 53234.

b. *Comment:* Several commenters asked whether systems that determine eligibility of clients for insurance coverage under broad categories such as medical coverage groups are considered health information. One commenter asked that we specifically exclude eligibility information from the standards.

Response: We cannot accept the latter suggestion. Eligibility information will typically be individually identifiable, and much eligibility information will also contain health information. If the information is ''individually identifiable'' and is ''health information,'' (with three very specific exceptions noted in the general discussion above) and it is in electronic form, it is covered by the security standards if maintained or transmitted by a covered entity.

c. *Comment:* Several commenters requested clarification as to whether the standards apply to identifiable health information in paper form. Some commenters believed the rule should be applicable to paper; others argued that it should apply to all confidential, identifiable health information.

Response: While we agree that protected health information in paper or other form also should have appropriate security protections, the proposed rule proposing the security standards proposed to apply those standards to health information in electronic form only. We are, accordingly, not extending the scope in this final rule.

We may establish standards to secure protected health information in other media in a future rule, in accordance with our statutory authority to do so. See discussion, supra, responding to a comment on the definition of ''health information'' and ''individually identifiable health information.''

d. *Comment:* The proposed rule would have excluded ''telephone voice response'' and ''faxback'' systems from the security standards, and we specifically solicited comments on that issue. A number of commenters agreed that telephone voice response and faxback should be excluded from the regulation, suggesting that the privacy standards rather than the security standards should apply. Others wanted those systems included, on the grounds that inclusion is necessary for consistency and in keeping with the intent of the Act. Still others specifically wanted personal computer-fax transmissions included. One commenter asked for clarification of when we would cover faxes, and another commenter asked why we were excluding them. Several commenters suggested that the other security requirements provide for adequate security of these systems.

Response: In light of these comments, we have decided that telephone voice response and ''faxback'' (that is, a request for information from a computer made via voice or telephone keypad input with the requested information returned as a fax) systems fall under this rule because they are used as input and output devices for computers, not because they have computers in them. Excluding these features would provide a huge loophole in any system concerned with security of the information contained and/or processed therein. It should be noted that employment of telephone voice response and/or faxback systems will generally require security protection by only one of the parties involved, and not the other. Information being transmitted via a telephone (either by voice or a DTMP tone pad) is not in electronic form (as defined in the first paragraph of the definition of ''electronic media'') before transmission and therefore is not subject to the Security Rule. Information being returned via a telephone voice response system in response to a telephone request is data that is already in electronic form and stored in a computer. This latter transmission does require protection under the Security Rule.

Although most recently made electronic devices contain microprocessors (a form of computer) controlled by firmware (an unchangeable form of computer program), we intend the term ''computer'' to include only software programmable computers, for example, personal computers, minicomputers, and mainframes. Copy machines, fax machines, and telephones, even those that contain memory and can produce multiple copies for multiple people are not intended to be included in the term ''computer.'' Therefore, because ''paper-to-paper'' faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this rule. See also the definition of ''electronic media'' at § 160.103.

We note that this guidance differs from the guidance regarding the applicability of the Transactions Rule to faxback and voice response systems. HHS has stated that faxback and voice response systems are not required to follow the standards mandated in the Transactions Rule. This new guidance refers only to this rule.

e. *Comment:* One commenter asked whether there is a need to implement special security practices to address the shipping and receiving of health information and asked that we more fully explain our expectations and solutions in the final rules.

Response: If the handling of electronic protected health information involves shipping and receiving, appropriate measures must be taken to protect the information. However, specific solutions are not provided within this rule, as discussed in section III.A.3 of this final rule. The device and media controls standard under § 164.310(d)(1) addresses this situation.

f. *Comment:* One commenter wanted the ''HTML'' statement reworded to eliminate a specific exemption for HTML from the regulation.

Response: The Transactions Rule did not adopt the proposed exemption for HTML. The use of HTML or any other electronic protocol is not exempt from the security standards. Generally, if protected health information is contained in any form of electronic transmission, it must be appropriately safeguarded.

g. *Comment:* One commenter asked to what degree ''family history'' is considered health information under this rule and what protections apply to family members included in a patient's family history.

Response: Any health-related ''family history'' contained in a patient's record that identifies a patient, including a person other than the patient, is individually identifiable health information and, to the extent it is also electronic protected health information, must be afforded the security protections.

h. *Comment:* Two commenters asked that the rule prohibit re-identification of de-identified data. In contrast, several commenters asked that we identify a minimum list or threshold of specific re-identification data elements (for example, name, city, and ZIP) that would fall under this final rule so that, for example, the rule would not affect numerous systems, for example, network adequacy and population-based clinical analysis databases. One commenter asked that we establish a means to use re-identified information if the entity already has access to the information or is authorized to have access.

Response: The issue of re-identification is addressed in the Privacy Rule at § 164.502(d) and § 164.514(c). The reader is referred to those sections and the related discussion in the preamble to the Privacy Rule (65 FR 82712) and the preamble to the Privacy Modifications (67 FR 53232 through 53234) for a full discussion of the issues of re-identification. We note that once information in the possession (or constructive possession) of a covered entity is re-identified and meets the definition of electronic protected health information, the security standards apply.

2. Technology-Neutral Standards

Comment: Many commenters expressed support for our efforts to develop standards for the security of health information. A number of comments were made in support of the technology-neutral approach of the proposed rule. For example, one commenter stated, ''By avoiding prescription of the specific technologies health care entities should use to meet the law's requirements, you are opening the door for industry to apply innovation. Technologies that don't currently exist or are impractical today could, in the near future, enhance health information security while minimizing the overall cost.'' Several other commenters stated that the requirements should be general enough to withstand changes to technology without becoming obsolete. One commenter anticipates no problems with meeting the standards.

In contrast, one commenter suggested that whenever possible, specific technology recommendations should provide sufficient detail to promote systems interoperability and decrease the tendency toward adoption of multiple divergent standards. Several commenters stated that by letting each organization determine its own rules, the rules impose procedural burdens without any substantive benefit to security.

Response: The overwhelming majority of comments supported our position. We do not believe it is appropriate to make the standards technology-specific because technology is simply moving too fast, for example, the increased use and sophistication of internet-enabled hand held devices. We believe that the implementation of these rules will promote the security of electronic protected health information by (1) providing integrity and confidentiality; (2) allowing only authorized individuals access to that information; and (3) ensuring its availability to those authorized to access the information. The standards do not allow organizations to make their own rules, only their own technology choices.

3. Miscellaneous Comments

a. *Comment:* Some commenters stated that the requirements and implementation features set out in the proposed rule were not specific enough to be considered standards, and that the actual standards are delegated to the discretion of the covered entities, at the expense of medical record privacy. Several commenters stated that it was inappropriate to balance the interests of those seeking to use identifiable medical information without patient consent against the interest of patients. Several other commenters believe that allowing covered entities to make their own decisions about the adequacy and balance of security measures undermined patient confidentiality interests, and stated that the proposed rule did not appear to adequately consider patient concerns and viewpoints.

Response: Again, the overwhelming majority of commenters supported our approach. This final rule sets forth requirements with which covered entities must comply and labels those requirements as standards and implementation specifications. Adequate implementation of this final rule by covered entities will ensure that the electronic protected health information in a covered entity's care will be as protected as is feasible for that entity.

We disagree that covered entities are given complete discretion to determine their security polices under this rule, resulting in effect, in no standards. While cost is one factor a covered identity may consider in determining whether to implement a particular implementation specification, there is nonetheless a clear requirement that adequate security measures be implemented, see 45 CFR 164.306(b). Cost is not meant to free covered entities from this responsibility.

b. *Comment:* Several commenters requested we withdraw the regulations, citing resource shortages due to Y2K preparation, upcoming privacy legislation, and/or the ''excessive micro-management'' contained in the rules. One commenter stated that, to insurers, these rules were onerous, not necessary, and not justified as cost-effective, as they already have effective practices for computer security and are subject to rigorous State laws for the safeguarding of health information. Another

commenter stated that these rules would adversely affect a provider's practice environment.

Response: The HIPAA statute requires us to promulgate a rule adopting security standards for health information. Resource concerns due to Y2K should no longer be an issue. Covered entities will have 2 years (or, in the case of small health plans, 3 years) from the adoption of this final rule in which to comply. Concerns relative to effective and compliance dates and the Privacy Rule are discussed under § 164.318, Compliance dates for initial implementation, below and at 65 FR 82751 through 82752.

We disagree that these standards will adversely affect a provider's practice environment. The scalability of the standards allows each covered entity to implement security protections that are appropriate to its specific needs, risks, and environments. These protections are necessary to maintain the confidentiality, integrity, and availability of patient data. A covered entity that lacks adequate protections risks inadvertent disclosure of patient data, with resulting loss of public trust, and potential legal action. For example, a covered entity with poor facility access controls and procedures would be susceptible to hacking of its databases. A provider with appropriate security protections already in place would only need to ensure that the protections are documented and are reassessed periodically to ensure that they continue to be appropriate and are actually being implemented. Our decision to classify many implementation specifications as addressable, rather than mandatory, provides even more flexibility to covered entities to develop cost-effective solutions. We believe that insurers who already have effective security programs in place will have met many of the requirements of this regulation.

c. *Comment:* One commenter believes the rule is arbitrary and capricious in its requirements without any justification that they will significantly improve the security of medical records and with the likelihood that their implementation may actually increase the vulnerability of the data. The commenter noted that the data backup requirements increase access to data and that security awareness training provides more information to employees.

Response: The standards are based on generally accepted security procedures, existing industry standards and guidelines, and recommendations contained in the National Research Council's 1997 report *For The Record: Protecting Electronic Health Information,* Chapter 6. We also consulted extensively with experts in the field of security throughout the health care industry. The standards are consistent with generally accepted security principles and practices that are already in widespread use.

Data backup need not result in increased access to that data. Backups should be stored in a secure location with controlled access. The appropriate secure location and access control will vary, based upon the security needs of the covered entity. For example, a procedure as simple as locking backup diskettes in a safe place and restricting who has access to the key may be suitable for one entity, whereas another may need to store backed-up information off-site in a secure computer facility. The information provided in security awareness training heightens awareness of security anomalies and helps to prevent security incidents.

d. *Comment:* Several commenters suggested that the proposed rule appears to reflect the Medicare program's perspective on security risks and solutions, and that it should be noted that not all industry segments share all the same risks as Medicare. One commenter stated that as future proposed rules are drafted, we should solicit input from those most significantly affected, for example, providers, plans, and clearinghouses.

Others stated that Medicaid agencies were not sufficiently involved in the discussions and debate. Still another stated that States would be unable to perform some basic business functions if all the standards are not designed to meet their needs.

Response: We believe that the standards are consistent with common industry practices and equitable, and that there has been adequate consultation with interested parties in the development of the standards. These standards are the result of an intensive process of public consultation. We consulted with the National Uniform Billing Committee, the National Uniform Claim Committee, the American Dental Association, and the Workgroup for Electronic Data Interchange, in the course of developing the proposed rule. Those organizations were specifically named in the Act to advise the Secretary, and their membership is drawn from the full spectrum of industry segments. In addition, the National Committee on Vital and Health Statistics (NCVHS), an independent advisory group to the Secretary, held numerous public hearings to obtain the views of interested parties. Again, many segments of the health care industry, including provider groups, health plans, clearinghouses, vendors, and government programs participated actively. The NCVHS developed recommendations to the Secretary, which were relied upon as we developed the proposed rule. Finally, we note that the opportunity to comment was available to all during the public comment period.

e. *Comment:* One commenter stated that there is a need to ensure the confidentiality of risk analysis information that may contain sensitive information.

Response: The information included in a risk analysis would not be subject to the security standards if it does not include electronic protected health information. We agree that risk analysis data could contain sensitive information, just as other business information can be sensitive. Covered entities may wish to develop their own business rules regarding access to and protections for risk analysis data.

f. *Comment:* One commenter expressed concern over the statement in the preamble of the proposed rule (63 FR 43250) that read: ''No one item is considered to be more important than another.'' The commenter suggested that security management should be viewed as most critical and perhaps what forms the foundation for all other security actions.

Response: The majority of comments received on this subject requested that we prioritize the standards. In response, we have regrouped the standards and implementation specifications in what we believe is a logical order within each of three categories: ''Administrative safeguards,'' ''Physical safeguards,'' and ''Technical safeguards.'' In this final rule, we order the standards in such a way that the ''Security management process'' is listed first under the ''Administrative safeguards'' section, as we believe this forms the foundation on which all of the other standards depend. The determination of the specific security measures to be implemented to comply with the standards will, in large part, be dependent upon completion of the implementation specifications within the security management process standard (see § 164.308(a)(1)). We emphasize, however, that an entity implementing these standards may choose to implement them in any order, as long as the standards are met.

g. *Comment:* One commenter stated that there is a need for requirements concerning organizational practices (for example, education, training, and security and confidentiality policies), as

well as technical practices and procedures.

Response: We agree. Section 164.308 of this final rule describes administrative safeguards that address these topics. Section 164.308 requires covered entities to implement standards and required implementation specifications, as well as consider and implement, when appropriate and reasonable, addressable implementation specifications. For example, the security management process standard requires implementation of a risk analysis, risk management, a sanction policy, and an information system activity review. The information access management standard requires consideration, and implementation where appropriate and reasonable, of access authorization and access establishment and modification policies and procedures. Other areas addressed are assigned security responsibility, workforce security, security awareness and training, security incident procedures, contingency planning, business associate contracts, and evaluation.

h. *Comment:* One commenter stated that internal and external security requirements should be separated and dealt with independently.

Response: The presentation of the standards within this final rule could have been structured in numerous ways, including by addressing separate internal and external security standards. We chose the current structure as we considered it a logical breakout for purposes of display within this final rule. Under our structure a covered entity may apply a given standard to internal activities and to external activities. Had we displayed separately the standards for internal security and the standards for external security, we would have needed to describe a number of the standards twice, as many apply to both internal and external security. However, a given entity may address the standards in whatever order it chooses, as long as the standards are met.

i. *Comment:* Two commenters stated that the standards identified in Addendum 3 of the proposed rule may not all have matured to implementation readiness.

Response: Addendum 3 of the proposed rule cross-referred individual requirements on the matrix to existing industry standards of varying levels of maturity. Addendum 3 was intended to show what we evaluated in searching for existing industry standards that could be adopted on a national level. No one standard was found to be comprehensive enough to be adopted, and none were proposed as the standards to be met under the Security Rule.

j. *Comment:* One commenter suggested we include a revised preamble in the final publication. Another questioned how clarification of points in the preamble will be handled if the preamble is not part of the final regulation.

Response: Preambles to proposed rules are not republished in the final rule. The preamble in this final rule contains summaries of the information presented in the preamble of the proposed rule, summaries of the comments received during the public comment period, and responses to questions and concerns raised in those comments and a summary of changes made. Additional clarification will be provided by HHS on an ongoing basis through written documents and postings on HHS's websites.

k. *Comment:* One commenter asked that we clarify that no third party can require implementation of more security features than are required in the final rule, for example, a third party could not require encryption but may choose to accept it if the other party so desires.

Response: The security standards establish a minimum level of security to be met by covered entities. It is not our intent to limit the level of security that may be agreed to between trading partners or others above this floor.

l. *Comment:* One commenter asked how privacy legislation would affect these rules. The commenter inquired whether covered entities will have to reassess and revise actions already taken in the spirit of compliance with the security regulations.

Response: We cannot predict if or how future legislation may affect the rules below. At present, the privacy standards at subpart E of 42 CFR part 164 have been adopted, and this final rule is compatible with them.

m. *Comment:* One commenter stated that a data classification policy, that is a method of assigning sensitivity ratings to specific pieces of data, should be part of the final regulations.

Response: We did not adopt such a policy because this final rule requires a floor of protection of all electronic protected health information. A covered entity has the option to exceed this floor. The sensitivity of information, the risks to and vulnerabilities of electronic protected health information and the means that should be employed to protect it are business determinations and decisions to be made by each covered entity.

n. *Comment:* One commenter stated that this proposed rule conflicts with previously stated rules that acceptable ''standards'' must have been developed by ANSI-recognized Standards Development Organizations (SDOs).

Response: In general, HHS is required to adopt standards developed by ANSI-accredited SDOs when such standards exist. The currently existing security standards developed by ANSI-recognized SDOs are targeted to specific technologies and/or activities. No existing security standard, or group of standards, is technology-neutral, scaleable to the extent required by HIPAA, and broad enough to be adopted in this final rule. Therefore, this final rule adopts standards under section 1172(c)(2)(B) of the Act, which permits us to develop standards when no industry standards exist.

o. *Comment:* One commenter stated that this regulation goes beyond the scope of the law, unjustifiably extending into business practices, employee policies, and facility security.

Response: We do not believe that this regulation goes beyond the scope of the law. The law requires HHS to adopt standards for reasonable and appropriate security safeguards concerning such matters as compliance by the officers and employees of covered entities, protection against reasonably anticipated unauthorized uses and disclosures of health information, and so on. Such standards will inevitably address the areas the commenter pointed to.

The intent of this regulation is to provide standards for the protection of electronic protected health information in accordance with the Act. In order to do this, covered entities are required to implement administrative, physical, and technical safeguards. Those entities must ensure that data are protected, to the extent feasible, from inappropriate access, modification, dissemination, and destruction. As noted above, however, this final rule has been modified to increase flexibility as to how this protection is accomplished.

p. *Comment:* One commenter stated that all sections regarding confidentiality and privacy should be removed, since they do not belong in this regulation.

Response: As the discussion in section III.A above of this final rule makes clear, the privacy and security standards are very closely related. Section 1173(d)(2) of the Act specifically mentions ''confidentiality'' and authorizes uses and disclosures of information as part of what security safeguards must address. Thus, we cannot omit all references to confidentiality and privacy in discussions of the security standards.

However, we have relocated material that relates to both security and privacy (including definitions) to the general section of part 164.

q. *Comment:* One commenter asked that data retention be addressed more specifically, since this will become a significant issue over time. It is recommended that a national work group be convened to address this issue.

Response: The commenter's concern is noted. While the documentation relating to Security Rule implementation must be retained for a period of 6 years (see § 164.316(b)(2)), it is not within the scope of this final rule to address data retention time frames for administrative or clinical records.

r. *Comment:* One commenter stated that requiring provider practices to develop policies, procedures, and training programs and to implement record keeping and documentation systems would be tremendously resource-intensive and increase the costs of health care.

Response: We expect that many of the standards of this final rule are already being met in one form or another by covered entities. For example, as part of normal business operations, health care providers already take measures to protect the health information in their keeping. Health care providers already keep records, train their employees, and require employees to follow office policies and procedures. Similarly, health plans are already frequently required by State law to keep information confidential. While revisions to a practice's or plan's current activities may be necessary, the development of entirely new systems or procedures may not be necessary.

s. *Comment:* One commenter stated that there is no system for which risk has been eliminated and expressed concern over phrases such as covered entities must ''assure that electronic health information pertaining to an individual remains secure.''

Response: We agree with the commenter that there is no such thing as a totally secure system that carries no risks to security. Furthermore, we believe the Congress' intent in the use of the word ''ensure'' in section 1173(d) of the Act was to set an exceptionally high goal for the security of electronic protected health information. However, we note that the Congress also recognized that some trade-offs would be necessary, and that ''ensuring'' protection did not mean providing protection, no matter how expensive. See section 1173(d)(1)(A)(ii) of the Act. Therefore, when we state that a covered entity must ensure the safety of the information in its keeping, we intend that a covered entity take steps, to the best of its ability, to protect that information. This will involve establishing a balance between the information's identifiable risks and vulnerabilities, and the cost of various protective measures, and will also be dependent upon the size, complexity, and capabilities of the covered entity, as provided in § 164.306(b).

E. Administrative Safeguards (§ 164.308)

We proposed that measures taken to comply with the rule be appropriate to protect the health information in a covered entity's care. Most importantly, we proposed to require that both the measures taken and documentation of those measures be kept current, that is, reviewed and updated periodically to continue appropriately to protect the health information in the care of covered entities. We would have required the documentation to be made available to those individuals responsible for implementing the procedure.

We proposed a number of administrative requirements and supporting implementation features, and required documentation for those administrative requirements and implementation features.

In this final rule, we have placed these administrative standards in § 164.308. We have reordered them, deleted much of the detail of the proposed requirements, as discussed below, and omitted two of the proposed sets of requirements (system configuration requirements and a requirement for a formal mechanism for processing records) as discussed in paragraph 10 of the discussion of § 164.308 of section III.E. of this preamble. Otherwise, the basic elements of the administrative safeguards are adopted in this final rule as proposed.

1. Security Management Process (§ 164.308(a)(1)(i))

We proposed the establishment of a formal security management process to involve the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations. This process would include implementation features consisting of a risk analysis, risk management, and sanction and security policies.

We also proposed, in a separate requirement under administrative procedures, an internal audit, which would be an in-house review of the records of system activity (for example, logins, file accesses, and security incidents) maintained by an entity.

In this final rule, risk analysis, risk management, and sanction policy are adopted as required implementation specifications although some of the details are changed, and the proposed internal audit requirement has been renamed as ''information system activity review'' and incorporated here as an additional implementation specification.

a. *Comment:* Three commenters asked that this requirement be deleted. Two commenters cited this requirement as a possible burden. Several commenters asked that the implementation features be made optional.

Response: This standard and its component implementation specifications form the foundation upon which an entity's necessary security activities are built. See NIST SP 800–30, ''Risk Management Guide for Information Technology Systems,'' chapters 3 and 4, January 2002. An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities. Some form of sanction or punishment activity must be instituted for noncompliance. Indeed, we question how the statutory requirement for safeguards ''to ensure compliance * * * by a [covered entity's] officers and employees'' could be met without a requirement for a sanction policy. See section 1176(d)(2)(C) of the Act. Accordingly, implementation of these specifications remains mandatory. However, it is important to note that covered entities have the flexibility to implement the standard in a manner consistent with numerous factors, including such things as, but not limited to, their size, degree of risk, and environment. We have deleted the implementation specification calling for an organizational security policy, as it duplicated requirements of the security management and training standard.

We note that the implementation specification for a risk analysis at § 164.308(a)(1)(ii)(A) does not specifically require that a covered entity perform a risk analysis often enough to ensure that its security measures are adequate to provide the level of security required by § 164.306(a). In the proposed rule, an assurance of adequate security was framed as a requirement to keep security measures ''current.'' We continue to believe that security measures must remain current, and have added regulatory language in § 164.306(e) as a more precise way of communicating that security measures

in general that must be periodically reassessed and updated as needed.

The risk analysis implementation specification contains other terms that merit explanation. Under § 164.308(a)(1)(ii)(A), the risk analysis must look at risks to the covered entity's electronic protected health information. A thorough and accurate risk analysis would consider ''all relevant losses'' that would be expected if the security measures were not in place. ''Relevant losses'' would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures.

b. *Comment:* Relative to the development of an entity's sanction policy, one commenter asked that we describe the sanction penalties for breach of security. Another suggested establishment of a standard to which one's conduct could be held and adoption of mitigating circumstances so that the fact that a person acted in good faith would be a factor that could be used to reduce or otherwise minimize any sanction imposed. Another commenter suggested sanction activities not be implemented before the full implementation and testing of all electronic transaction standards.

Response: The sanction policy is a required implementation specification because—(1) the statute requires covered entities to have safeguards to ensure compliance by officers and employees; (2) a negative consequence to noncompliance enhances the likelihood of compliance; and (3) sanction policies are recognized as a usual and necessary component of an adequate security program. The type and severity of sanctions imposed, and for what causes, must be determined by each covered entity based upon its security policy and the relative severity of the violation.

c. *Comment:* Commenters requested the definitions of ''risk analysis'' and ''breach.''

Response: ''Risk analysis'' is defined and described in the specification of the security management process standard, and is discussed in the preamble discussion of § 164.308(a)(1)(ii)(A) of this final rule. The term breach is no longer used and is, therefore, not defined.

d. *Comment:* One commenter asked whether all health information is considered equally ''sensitive,'' the thought being that, in determining risk, an entity may consider the loss of a smaller amount of extraordinarily sensitive data to be more significant than the loss of a larger amount of routinely collected data. The commenter stated that common reasoning would suggest that the smaller amount of data would be considered more sensitive.

Response: All electronic protected health information must be protected at least to the degree provided by these standards. If an entity desires to protect the information to a greater degree than the risk analysis would indicate, it is free to do so.

e. *Comment:* One commenter asked that we add ''threat assessment'' to this requirement.

Response: We have not done this because we view threat assessment as an inherent part of a risk analysis; adding it would be redundant.

f. *Comment:* We proposed a requirement for internal audit, the in-house review of the records of system activity (for example, logins, file accesses, and security incidents) maintained by an entity. Several commenters wanted this requirement deleted. One suggested the audit trail requirement should not be mandatory, while another stated that internal audits would be unnecessary if physical security requirements are implemented.

A number of commenters asked that we clarify the nature and scope of what an internal audit covers and what the audit time frame should be. Several commenters offered further detail concerning what should and should not be required in an internal audit for security purposes. One commenter stated that ongoing intrusion detection should be included in this requirement. Another wanted us to specify the retention times for archived audit logs.

Several commenters had difficulty with the term ''audit'' and suggested we change the title of the requirement to ''logging and violation monitoring.''

A number of commenters stated this requirement could result in an undue burden and would be economically unfeasible.

Response: Our intent for this requirement was to promote the periodic review of an entity's internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity's security environment. The term ''internal audit'' apparently, based on the comments received, has certain rigid formal connotations we did not intend. We agree that the implementation of formal internal audits could prove burdensome or even unfeasible, to some covered entities due to the cost and effort involved. However, we do not want to overlook the value of internal reviews. Based on our review of the comments and the text to which they refer, it is clear that this requirement should be renamed for clarity and that it should actually be an implementation specification of the security management process rather than an independent standard. We accordingly remove ''internal audit'' as a separate requirement and add ''information system activity review'' under the security management process standard as a mandatory implementation specification.

2. Assigned Security Responsibility (§ 164.308(a)(2))

We proposed that the responsibility for security be assigned to a specific individual or organization to provide an organizational focus and importance to security, and that the assignment be documented. Responsibilities would include the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.

In this final rule, we clarify that the final responsibility for a covered entity's security must be assigned to one official. The requirement for documentation is retained, but is made part of § 164.316 below. This policy is consistent with the analogous policy in the Privacy Rule, at 45 CFR 164.530(a), and the same considerations apply. See 65 FR 82744 through 87445. The same person could fill the role for both security and privacy.

a. *Comment:* Commenters were concerned that delegation of assigned security responsibility, especially in large organizations, needs to be to more than a single individual. Commenters believe that a large health organization's security concerns would likely cross many departmental boundaries requiring group responsibility.

Response: The assigned security responsibility standard adopted in this final rule specifies that final security responsibility must rest with one individual to ensure accountability within each covered entity. More than one individual may be given specific security responsibilities, especially within a large organization, but a single individual must be designated as having the overall final responsibility for the security of the entity's electronic protected health information. This decision also aligns this rule with the final Privacy Rule provisions concerning the Privacy Official.

b. *Comment:* One commenter disagreed with placing assigned security responsibility as part of physical safeguards. The commenter suggested that assigned security responsibility should be included under the Administrative Procedures.

Response: Upon review of the matrix and regulations text, we agree with the commenter, because this requirement involves an administrative decision at the highest levels of who should be responsible for ensuring security measures are implemented and maintained. Assigned security responsibility has been removed from ''Physical safeguards'' and is now located under ''Administrative safeguards'' at § 164.308.

3. Workforce Security (§ 164.308(a)(3)(i))

We proposed implementation of a number of features for personnel security, including ensuring that maintenance personnel are supervised by a knowledgeable person, maintaining a record of access authorizations, ensuring that operating and maintenance personnel have proper access authorization, establishing personnel clearance procedures, establishing and maintaining personnel security policies and procedures, and ensuring that system users have proper training.

In this final rule, to provide clarification and reduce duplication, we have combined the ''Assure supervision of maintenance personnel by authorized, knowledgeable person'' implementation feature and the ''Operating, and in some cases, maintenance personnel have proper access authorization'' feature into one addressable implementation specification titled ''Authorization and/or supervision.''

In a related, but separate, requirement entitled ''Termination procedures,'' we proposed implementation features for the ending of an employee's employment or an internal or external user's access. These features would include things such as changing combination locks, removal from access lists, removal of user account(s), and the turning in of keys, tokens, or cards that allow access.

In this final rule, ''Termination procedures'' has been made an addressable implementation specification under ''Workforce security.'' This is addressable because in certain circumstances, for example, a solo physician practice whose staff consists only of the physician's spouse, formal procedures may not be necessary.

The proposed ''Personnel security policy/procedure'' and ''record of access authorizations'' implementation features have been removed from this final rule, as they have been determined to be redundant. Implementation of the balance of the ''Workforce security'' implementation specifications and the other standards contained within this final rule will result in assurance that all personnel with access to electronic protected health information have the required access authority as well as appropriate clearances.

a. *Comment:* The majority of comments concerned the supervision of maintenance personnel by an authorized knowledgeable person. Commenters stated this would not be feasible in smaller settings. For example, the availability of technically knowledgeable persons to ensure this supervision would be an issue. We were asked to either reword this implementation feature or delete it.

Response: We agree that a ''knowledgeable'' person may not be available to supervise maintenance personnel. We have accordingly modified this implementation specification so that, in this final rule, we are adopting an addressable implementation specification titled, ''Authorization and/or supervision,'' requiring that workforce members, for example, operations and maintenance personnel, must either be supervised or have authorization when working with electronic protected health information or in locations where it resides (see § 164.308(a)(3)(ii)(A)). Entities can decide on the feasibility of meeting this specification based on their risk analysis.

b. *Comment:* The second largest group of comments requested assurance that, with regard to the proposed ''Personnel clearance procedure'' implementation feature, having appropriate clearances does not mean performing background checks on everyone. We were asked to delete references to ''clearance'' and use the term ''authorization'' in its place.

Response: We agree with the commenters concerning background checks. This feature was not intended to be interpreted as an absolute requirement for background checks. We retain the use of the term ''clearance,'' however, because we believe that it more accurately conveys the screening process intended than does the term ''authorization.'' We have attempted to clarify our intent in the language of § 164.308(a)(3)(ii)(B), which now reads, ''Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.'' The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective personnel screening processes may be applied in a way to allow a range of implementation, from minimal procedures to more stringent procedures based on the risk analysis performed by the covered entity. So long as the standard is met and the underlying standard of § 164.306(a) is met, covered entities have choices in how they meet these standards. To clarify the intent of this provision, we retitle the implementation specification ''Workforce clearance procedure.''

c. *Comment:* One commenter asked that we expand the implementation features to include the identification of the restrictions that should be placed on members of the workforce and others.

Response: We have not adopted this comment in the interest of maintaining flexibility as discussed in § 164.306. Restrictions would be dependent upon job responsibilities, the amount and type of supervision required and other factors. We note that a covered entity should consider in this regard the applicable requirements of the Privacy Rule (*see*, for example, § 164.514(d)(2) (relating to minimum necessary requirements), and § 164.530(c) (relating to safeguards).

Comment: One commenter believes that the proposed ''Personnel security'' requirement was reasonable, since an administrative determination of trustworthiness is needed before allowing access to sensitive information. Two commenters asked that we delete the requirement entirely. A number of commenters requested that we delete the implementation features. Another commenter stated that all the implementation features may not be applicable or even appropriate to a given entity and should be so qualified.

Response: While we do not believe this requirement should be eliminated, we agree that all the implementation specifications may not be applicable or even appropriate to a given entity. For example, a personal clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse. The implementation specifications are not mandatory, but must be addressed. This final rule has been changed to reflect this approach (see § 164.308(a)(3)(ii)(B)).

e. *Comment:* The majority of commenters on the ''Termination procedures'' requirement asked that it be made optional, stating that it may not be applicable or even appropriate in all circumstances and should be so qualified or posed as guidelines. A number of commenters stated that the requirement should be deleted. One commenter stated that much of the material covered under the ''Termination procedures'' requirement is already covered in ''Information access control.'' A number of commenters stated that this requirement

was too detailed and some of the requirements excessive.

Response: Based upon the comments received, we agree that termination procedures should not be a separate standard; however, consideration of termination procedures remains relevant for any covered entity with employees, because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution or use of proprietary information for personal gain. We further agree with the reasoning of the commenters who asked that these procedures be made optional; therefore, ''Termination procedures'' is now reflected in this final rule as an addressable implementation specification. We also removed reference to all specific termination activities, for example, changing locks, because, although the activities may be considered appropriate for some covered entities, they may not be reasonable for others.

f. *Comment:* One commenter asked whether human resource employee termination policies and procedures must be documented to show the types of security breaches that would result in termination.

Response: Policies and procedures implemented to adhere to this standard must be documented (see § 164.316 below). The purpose of termination procedure documentation under this implementation specification is not to detail when or under which circumstances an employee should be terminated. This information would more appropriately be part of the entity's sanction policy. The purpose of termination procedure documentation is to ensure that termination procedures include security-unique actions to be followed, for example, revoking passwords and retrieving keys when a termination occurs.

4. Information Access Management (§ 164.308(a)(4))

We proposed an ''information access control'' requirement for establishment and maintenance of formal, documented policies and procedures defining levels of access for all personnel authorized to access health information, and how access is granted and modified. In § 164.308(a)(4)(ii)(B) and (C) below, the proposed implementation features are made addressable specifications. We have added in § 164.308(a)(4)(ii)(A), a required implementation specification to isolate health care clearinghouse functions to address the provisions of section 1173(d)(1)(B) of the Act which related to this area.

a. *Comment:* One commenter asked that the requirement be deleted, expressing the opinion that this requirement goes beyond ''reasonable boundaries'' into regulating common business practices. In contrast, another asked that we expand this requirement to identify participating parties and access privileges relative to specific data elements.

Response: We disagree that this requirement improperly imposes upon business functions. Restricting access to those persons and entities with a need for access is a basic tenet of security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is minimized. We cannot, however, specifically identify participating parties and access privileges relative to data elements within this regulation. These will vary depending upon the entity, the needs within the user community, the system in which the data resides, and the specific data being accessed. This standard is consistent with § 164.514(d) in the Privacy Rule (minimum necessary requirements for use and disclosure of protected health information), and is, therefore, being retained.

b. *Comment:* Several commenters asked that we not mandate the implementation features, but leave them as optional, a suggested means of compliance. The commenters noted that this might make the rules more scalable and flexible, since this approach would allow providers to implement safeguards that best addressed their needs. Along this line, one commenter expressed the belief that each organization should implement features deemed necessary based on its own risk assessment.

Response: While the information access management standard in this final rule must be met, we agree that the implementation specifications at § 164.308(a)(4)(ii)(B) and (C) should not be mandated but posed as a suggested means of compliance, which must be addressed. These specifications may not be applicable to all entities based on their size and degree of automation. A fully automated covered entity spanning multiple locations and involving hundreds of employees may determine it has a need to adopt a formal policy for access authorization, while a small provider may decide that a desktop standard operating procedure will meet the specifications. The final rule has been revised accordingly.

c. *Comment:* Clarification was requested concerning the meaning of ''formal.''

Response: The word ''formal'' has caused considerable concern among commenters, as it was thought ''formal'' carried the connotation of a rigidly defined structure similar to what might be found in the Department of Defense instructions. As used in the proposed rule, this word was not intended to convey such a strict structure. Rather, it was meant to convey that documentation should be an official organizational statement as opposed to word-of-mouth or cryptic notes scratched on a notepad. While documentation is still required (see § 164.316), to alleviate confusion, the word ''formal'' has been deleted.

d. *Comment:* One commenter asked that we clarify that this requirement relates to both the establishment of policies for the access control function and to access control (the implementation of those policies).

Response: ''Information access management'' does address both the establishment of access control policies and their implementation. We use the term ''implement'' to clarify that the procedures must be in use, and we believe that the requirement to implement policies and procedures requires, as an antecedent condition, the establishment or adaptation of those policies and procedures.

5. Security Awareness and Training (§ 164.308(a)(5)(i))

We proposed, under the requirement ''Training,'' that security training be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.

In this final rule, we adopt this proposed requirement in modified form. For the standard ''Security awareness and training,'' in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The ''Virus protection'' implementation feature has been renamed ''protection from malicious software,'' because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms.

a. *Comment:* One commenter believes that security awareness training for all

system users would be too difficult to do in a large organization.

Response: We disagree with the commenter. Security awareness training is a critical activity, regardless of an organization's size. This feature would typically become part of an entity's overall training program (which would include privacy and other information technology items as well). For example, the Government Information Systems Reform ACT (GISRA) of 2000 requires security awareness training as part of Federal agencies' information security programs, including Federal covered entities, such as the Medicare program. In addition, National Institute of Standards and Technology (NIST) SP 800–16, *Information Technology Security Training Requirements, A role and performance base model, April 1998,* provides an excellent source of information and guidance on this subject and is targeted at industry as well as government activities. We also note that covered entities must have discretion in how they implement the requirement, so they can incorporate this training in other existing activities. One approach would be to require this training as part of employee orientation.

b. *Comment:* A number of commenters asked that this requirement be made optional or used as a guideline only. Several commenters stated that this requirement is too specific and is burdensome. Several asked that the implementation features be removed.

Several others stated that this requirement is not appropriate for agents or contractors. One commenter asked how to apply this requirement to outsiders having access to data. Another asked if this requirement included all subcontractor staff. Others stated that contracts, signed by entities such as consultants, that address training should be sufficient.

Response: Security training remains a requirement because of its criticality; however, we have revised the implementation specifications to indicate that the amount and type of training needed will be dependent upon an entity's configuration and security risks. Business associates must be made aware of security policies and procedures, whether through contract language or other means. Covered entities are not required to provide training to business associates or anyone else that is not a member of their workforce.

c. *Comment:* Several commenters questioned why security awareness training appeared in two places, under ''Physical safeguards'' as well as ''Administrative safeguards.'' Others questioned the appropriateness of security awareness training under ''Physical safeguards.''

Response: We reviewed the definitions of the proposed ''Awareness training for all personnel'' (''Administrative safeguards'') implementation feature and the proposed ''Security awareness training'' (''Physical safeguards'') requirement. We agree that, to avoid confusion and eliminate redundancy, security awareness and training should appear in only one place. We believe the appropriate location for it is under ''Administrative safeguards,'' as such training is essentially an administrative function.

d. *Comment:* Several commenters objected to the blanket requirement for security awareness training of individuals who may be on site for a limited time period (for example, a single day).

Response: Each individual who has access to electronic protected health information must be aware of the appropriate security measures to reduce the risk of improper access, uses, and disclosures. This requirement does not mean lengthy training is appropriate in every instance; there are alternative methods to inform individuals of security responsibilities (for example, provisions of pamphlets or copies of security policies, and procedures).

e. *Comment:* One commenter asked that ''training'' be changed to ''orientation.''

Response: We believe the term ''training,'' as presented within this rule is the more appropriate term. The rule does not contemplate a one-time type of activity as connoted by ''orientation,'' but rather an on-going, evolving process as an entity's security needs and procedures change.

f. *Comment:* Several commenters asked how often training should be conducted and asked for a definition of ''periodic,'' as it appears in the proposed implementation feature ''Periodic security reminders.'' One asked if the training should be tailored to job need.

Response: Amount and timing of training should be determined by each covered entity; training should be an on-going, evolving process in response to environmental and operational changes affecting the security of electronic protected health information. While initial training must be carried out by the compliance date, we provide flexibility for covered entities to construct training programs. Training can be tailored to job need if the covered entity so desires.

6. Security Incident Procedures (§ 164.308(a)(6))

We proposed a requirement for implementation of accurate and current security incident procedures: formal, documented report and response procedures so that security violations would be reported and handled promptly. We adopt this standard in the final rule, along with an implementation specification for response and reporting, since documenting and reporting incidents, as well as responding to incidents are an integral part of a security program.

a. *Comment:* Several commenters asked that we further define the scope of a breach of security. Along this same line, another commenter stated that the proposed security incident procedures were too vague as stated. We were asked to specify what a security incident would be, what the internal chain for reporting procedures would be, and what should be included in the documentation (for example, hardware/software, personnel responses).

Response: We define a security incident in § 164.304. Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with the other security standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations.

b. *Comment:* One commenter asked what types of incidents must be reported to outside entities. Another commented that we clarify that incident reporting is internal.

Response: Internal reporting is an inherent part of security incident procedures. This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations.

c. *Comment:* One commenter stated that network activity should be included here.

Response: We see no reason to exclude network activity under this requirement. Improper network activity should be treated as a security incident, because, by definition, it represents an improper instance of access to or use of information.

d. *Comment:* One commenter stated that this requirement should address suspected misuse also.

Response: We agree that security incidents include misuse of data; therefore, this requirement is addressed.

e. *Comment:* Several commenters asked that this requirement be deleted. One commenter asked that we delete the implementation features.

Response: As indicated above, we have adopted the proposed standard and combined the implementation specifications.

7. Contingency Plan (§ 164.308(a)(7)(i))

We proposed that a contingency plan must be in effect for responding to system emergencies. The plan would include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.

In this final rule, we make the implementation specifications for testing and revision procedures and an applications and data criticality analysis addressable, but otherwise require that the contingency features proposed be met.

a. *Comment:* Several commenters suggested the contingency plan requirement be deleted. Several thought that this aspect of the proposed regulation went beyond its intended scope. Another believed that more discussion and development is needed before developing regulatory guidance on contingency plans. Others wanted this to be an optional requirement. In contrast, one commenter requested more guidance concerning contingency planning. Still others wanted to require that a contingency plan be in place but stated that we should not regulate its contents. One comment stated that data backup, disaster recovery, and emergency mode operation should not be part of this requirement.

Response: A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.

Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.

While the contingency plan standard must be met, we agree that the proposed testing and revision implementation feature should be an addressable implementation specification in this final rule. Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach.

b. *Comment:* One commenter believed that adhering to this requirement could prove burdensome. Another stated that testing of certain parts of a contingency plan would be burdensome, and even infeasible, for smaller entities.

Response: Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)).

c. *Comment:* Two commenters considered a 2-year implementation time frame for this requirement inadequate for large health plans. Another commenter stated that implementation of measures against natural disaster would be too big an issue for this regulation.

Response: The statute sets forth the compliance dates for the initial standards. The statute requires that compliance with initial standards is not later than 2 years after adoption of the standards for all covered entities except small health plans for which the compliance date is not later than 3 years after adoption.

The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.

d. *Comment:* A commenter requested clarification of the term ''Emergency mode'' with regard to the proposed ''Emergency mode operation plan'' implementation feature.

Response: We have clarified the ''Emergency mode operations plan'' to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

8. Evaluation (§ 164.308(a)(8))

We proposed that certification would be required and could be performed internally or by an external accrediting agency. We solicited input on appropriate mechanisms to permit an independent assessment of compliance. We were particularly interested in input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation. We also solicited comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

In this final rule, we require covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.

a. *Comment:* We received several comments that certification should be performed externally. A larger group of commenters preferred self-certification. The majority of the comments, however, were to the effect that external certification should be encouraged but not mandated.

A number of commenters thought that mandating external certification would create an undue financial burden, regardless of the size of the entity being certified. One commenter stated that external certification would not place an undue burden on a small or rural provider.

Response: Evaluation by an external entity is a business decision to be left to each covered entity. Evaluation is required under § 164.308(a)(8), but a covered entity may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.

b. *Comment:* Several commenters stated that the certification should cover all components of the proposed rule, not just the information systems.

Response: We agree. We have revised this section to reflect that evaluation would be both technical and nontechnical components of security.

c. *Comment:* A number of commenters expressed a desire for the creation of certification guides or models to complement the rule.

Response: We agree that creation of compliance guidelines or models for different business environments would help in the implementation and evaluation of HIPAA security requirements and we encourage professional associations and others to do so. We may develop technical assistance materials, but do not intend to create certification criteria because we do not have the resources to address the large number of different business environments.

d. *Comment:* Some commenters asked how certification is possible without specifying the level of risk that is permissible.

Response: The level of risk that is permissible is specified by § 164.306(a). How such risk is managed will be determined by a covered entity through its security risk analysis and the risk mitigation activities it implements in order to ensure that the level of security required by § 164.306 is provided.

e. *Comment:* Several commenters requested creation of a list of Federally ''certified'' security software and off-the-shelf products. Several others stated that this request was not feasible. Regarding certification of off-the-shelf products, one commenter thought this should be encouraged, but not mandated; several thought this would be an impractical endeavor.

Response: While we will not assume the task of certifying software and off-the-shelf products for the reason described above, we have noted with interest that other Government agencies such as the National Institute of Standards and Technology (NIST) are working towards that end. The health care industry is encouraged to monitor the activity of NIST and provide comments and suggestions when requested (see *http://www.niap.nist.gov.*).

f. *Comment:* One commenter stated, ''With HCFA's publishing of these HIPAA standards, and their desire to retain the final responsibility for determining violations and imposing penalties of the statute, it also seems appropriate for HCFA to also provide certifying services to ensure security compliance.''

Response: In view of the enormous number and variety of covered entities, we believe that evaluation can best be handled through the marketplace, which can develop more usable and targeted evaluation instruments and processes.

8. Business Associate Contracts or Other Arrangements (§ 164.308(b)(1))

In the proposed rule § 142.308(a)(2) ''Chain of trust'' requirement, we proposed that covered entities be required to enter into a chain of trust partner agreement with their business partners, in which the partners would agree to electronically exchange data and protect the integrity, confidentiality, and availability of the data exchanged. This standard has been modified from the proposed requirement to reflect, in § 164.308(b)(1) ''Business associate contracts and other arrangements,'' the business associate structure put in place by the Privacy Rule.

In this final rule, covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in § 160.103. The covered entity must obtain satisfactory assurances from the business associate that it will appropriately safeguard the information in accordance with these standards (see § 164.314(a)(1)).

The comments received on the proposed chain of trust partner agreements are discussed in section 2 ''Business associate contracts and other arrangements'' of the discussion of § 164.314 below.

9. Proposed Requirements Not Adopted in This Final Rule

a. Security Configuration Management

We proposed that an organization would be required to implement measures, practices, and procedures regarding security configuration management. They would be coordinated and integrated with other system configuration management practices for the security of information systems. These would include documentation, hardware and/or software installation and maintenance review and testing for security features, inventory procedures, security testing, and virus checking.

Comment: Several commenters asked that the entire requirement be deleted. Several others asked that the inventory and virus checking implementation features be removed as they believe those features are not germane to security configuration management. A number of commenters requested that security testing be deleted because this implementation feature is too detailed, unreasonable, impractical, and beyond the scope of the legislation. Others stated that the testing would be very complex and expensive. Others wanted more clarification of what we intend by security testing, and how much would be enough. A number of commenters asked that all of the implementation features be deleted. Others asked that the implementation features be made optional. Several commenters wanted to know the scope of organizational integration required. Several others asked if what we meant by Security Configuration Management was change or version control.

Response: Upon review, this requirement appears unnecessary because it is redundant of other requirements we are adopting in this rule. A covered entity will have addressed the activities described by the features under this proposed requirement by virtue of having implemented the risk analysis, risk management measures, sanction policies, and information systems criticality review called for under the security management process. The proposed documentation implementation feature has been made a separate standard (see § 164.316). As a result, the Security Configuration Management requirement is not adopted in this final rule.

b. Formal Mechanism for Processing Records

The proposed rule proposed requiring a formal mechanism for processing records, and documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. This requirement has not been adopted in the final rule.

Comment: Several commenters thought this requirement concerned the regulation of formal procedures for how an entity does business and stated that such procedures should not be regulated. Others asked for additional clarification of what is meant by this requirement. One commenter thought the requirement too ambiguous and asked for clarification as to whether we meant such things as ''the proper handling of storage media, databases, transmissions,'' or ''the clinical realm of processes.''

Two commenters asked how extensive this requirement would be and whether systems' user manuals and policies and procedures for handling health information would suffice and what level of detail would be expected.

Several thought this requirement could result in a significant resource and monetary burden to develop and maintain formal procedures. Two asked for an explanation of the benefit to be derived from this requirement.

One asked that covered entities be required to document processes that create a security risk only and suggested that a risk assessment would determine the need for this documentation.

Response: We agree with the commenters that the standard is ambiguous, and upon review, is unnecessary because the remaining standards, for example, device and media controls, provide adequate safeguards. Accordingly, this requirement is not adopted in this final rule.

F. Physical Safeguards (§ 164.310)

We proposed requirements and implementation features for documented physical safeguards to guard data integrity, confidentiality, and availability. We proposed to require safeguards in the following areas: Assigned security responsibility; media controls; physical access controls; policies and guidelines on workstation use; a secure workstation location; and security awareness training. A number of specific implementation features were proposed under the media controls and physical access controls requirements.

In § 164.310 of this final rule, most of the proposed implementation features are adopted as addressable implementation specifications. The proposed requirements for the assigned security responsibility and security awareness training requirements are relocated in § 164.308.

1. General Comments

a. *Comment:* Several commenters made suggestions to modify the language to more clearly describe ''Physical safeguards.''

Response: In response to comments, we have revised the definition of ''Physical safeguards'' to read as follows: ''Physical safeguards are security measures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.''

b. *Comment:* One commenter was concerned that electronic security systems could not be used in lieu of physical security systems.

Response: This final rule does not preclude the use of electronic security systems in lieu of, or in combination with, physical security systems to meet a ''Physical safeguard'' standard.

2. Facility Access Controls (§ 164.310(a)(1))

We proposed, under the ''Physical access controls'' requirement, formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. These controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into and out of site), a facility security plan, procedures for verifying access authorizations before physical access, maintenance records, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision.

In § 164.310(a)(2) below, we combine and restate these as addressable implementation specifications. These are contingency operations, facility security plan, access control and validation procedures, and maintenance records.

a. *Comment:* Many commenters were concerned because the proposed language would require implementation of all physical access control features. Other commenters were concerned that the language did not allow entities to use the results of their risk assessment and risk management process to arrive at the appropriate solutions for them.

Response: We agree that implementation of all implementation specifications may not be appropriate in all situations. While the facility access controls standard must be met, we agree that the implementation specifications should not be required in all circumstances, but should be addressable. In this final rule, all four implementation specifications are addressable.

We have also determined, based on ''level of detail'' comments requesting consolidation of the list of implementation features, that the proposed implementation feature ''Equipment control (into and out of site)'' was redundant. ''Equipment control'' is already covered under the ''Device and media controls'' standard at § 164.310(d)(1). Accordingly, we have eliminated it as a separate implementation specification.

b. *Comment:* One commenter raised the issue of a potential conflict of authority between those having access to the data and those responsible for checking and maintaining access controls.

Response: Any potential conflicts should be identified, addressed, and resolved in the policies and procedures developed according to the standards under § 164.308.

c. *Comment:* Several commenters questioned whether ''Physical Access Controls'' was a descriptive phrase to describe a technology to be used, or whether the phrase referred to a facility.

Response: We agree that the term ''Physical'' may be misleading; to remove any confusion, the requirement is reflected in this final rule as a standard titled ''Facility access controls.'' We believe this is a more precise term to describe that the standard, and its associated implementation specifications, is applicable to an entity's business location or locations.

d. *Comment:* Several commenters requested that the disaster recovery and emergency mode operations features be moved to ''Administrative safeguards.'' Other commenters recommended that disaster recovery and emergency mode operations should be replaced by, and included in, a ''Contingency Operations'' implementation feature.

Response: The ''Administrative safeguards'' section addresses the contingency planning that must be done to contend with emergency situations. The placement of the disaster recovery and emergency mode operations implementation specifications in the ''Physical safeguards'' section is also appropriate, however, because ''Physical safeguards'' defines the physical operations (processes) that provide access to the facility to implement the associated plans, developed under § 164.308. We agree, however, that the term ''contingency operations'' better describes, and would include, disaster recovery and emergency mode operations, and have modified the regulation text accordingly (see § 164.310(a)(1)).

e. *Comment:* Commenters were concerned about having to address in their facility security plan the exterior/interior security of a building when they are one of many occupants rather than the sole occupant. Additional commenters were concerned that the responsibility for physical security of the building could not be delegated to a third party when the covered entity shares the building with other offices.

Response: The facility security plan is an addressable implementation specification. However, the covered entity retains responsibility for considering facility security even where it shares space within a building with other organizations. Facility security measures taken by a third party must be considered and documented in the covered entity's facility security plan, when appropriate.

3. Workstation Use (§ 164.310(b))

We proposed policy and guidelines on workstation use that included documented instructions/procedures delineating the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize the security of health information. In this final rule, we adopt this standard.

Comment: One commenter was concerned most people may be misled by the use of ''terminal'' as an example in the definition of workstation. The concern was that the standard only addresses ''fixed location devices,'' while in many instances the workstation has become a laptop computer.

Response: For clarity, we have added the definition of ''workstation'' to § 164.304 and deleted the word ''terminal'' from the description of workstation use in § 164.310(b).

4. Workstation Security (§ 164.310(c))

We proposed that each organization would be required to put in place physical safeguards to restrict access to information. In this final rule, we retain the general requirement for a secure workstation.

Comment: Comments were directed toward the example profiled in the definition of a secure workstation location. It was believed that what constitutes a secure workstation location must be dependent upon the entity's risk management process.

Response: We agree that what constitutes an appropriate solution to a covered entity's workstation security issues is dependent on the entity's risk analysis and risk management process. Because many commenters incorrectly interpreted the examples as the required and only solution for securing the workstation location, we have modified the regulations text description to generalize the requirement (see § 164.310(c)). Also, for clarity, the title ''Secure workstation location'' has been changed to ''Workstation security'' (see also the definition of ''Workstation'' at § 164.304).

5. Device and Media Controls (§ 164.310(d)(1))

We proposed that covered entities have media controls in the form of formal, documented policies and procedures that govern the receipt and removal of hardware and/or software (for example, diskettes and tapes) into and out of a facility. Implementation features would have included ''Access control,'' ''Accountability'' (tracking mechanism), ''Data backup,'' ''Data storage,'' and ''Disposal.''

In this final rule, we adopt most of these provisions as addressable implementation specifications and add a specification for media re-use. We change the name from ''Media controls'' to ''Device and media controls'' to more clearly reflect that this standard concerns hardware as well as electronic media. The proposed ''Access control'' implementation feature has been removed, as it is addressed as part of other standards (see section III.C.12.c of this preamble).

a. *Comment:* One commenter was concerned about the exclusion of removable media devices from examples of physical types of hardware and/or software.

Response: The media examples used were not intended to represent all possible physical types of hardware and/or software. Removable media devices, although not specifically listed, are not intended to be excluded.

b. *Comment:* Comments were made that the issue of equipment re-use or recycling of media containing mass storage was not addressed in ''Media controls.''

Response: We agree that equipment re-use or recycling should be addressed, since this equipment may contain electronic protected health information. The ''Device and media controls'' standard is accordingly expanded to include a required implementation specification that addresses the re-use of media (see § 164.310(d)(2)(ii)).

c. *Comment:* Several commenters asked for a definition of the term ''facility,'' as used in the proposed ''Media controls'' requirement description. Commenters were unclear whether we were talking about a corporate entity or the physical plant.

Response: The term ''facility'' refers to the physical premises and the interior and exterior of a building(s). We have added this definition to § 164.304.

d. *Comment:* Several commenters believe the ''Media controls'' implementation features are too onerous and should be deleted.

Response: While the ''Device and media controls'' standard must be met, we believe, based upon further review, that implementation of all specifications would not be necessary in every situation, and might even be counter-productive in some situations. For example, small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large health care providers or health plans. We have, therefore, reclassified the ''Accountability and data backup'' implementation specification as addressable to provide more flexibility in meeting the standard.

e. *Comment:* One commenter was concerned about the accountability impact of audit trails on system resources and the pace of system services.

Response: The proposed audit trail implementation feature appears as the addressable ''Accountability'' implementation specification. The name change better reflects the purpose and intended scope of the implementation specification. This implementation specification does not address audit trails within systems and/or software. Rather it requires a record of the actions of a person relative to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person. The impact of maintaining accountability on system resources and services will depend upon the complexity of the mechanism to establish accountability. For example, the appropriate mechanism for a given entity may be manual, such as receipt and removal restricted to specific persons, with logs kept. Maintaining accountability in such a fashion should have a minimal, if any, effect on system resources and services.

f. *Comment:* A commenter was concerned about the resource expenditure (system and fiscal) for total e-mail backup and wanted a clarification of the extensiveness of data backup.

Response: The data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. The data backup plan, which is part of the required contingency plan (see § 164.308(a)(7)(ii)(A)), should define exactly what information is needed to be retrievable to allow the entity to continue business ''as usual'' in the face of damage or destruction of data, hardware, or software. The extent to which e-mail backup would be needed would be determined through that analysis.

G. Technical Safeguards (§ 164.312)

We proposed five technical security services requirements with supporting implementation features: Access control; Audit controls; Authorization control; Data authentication; and Entity authentication. We also proposed specific technical security mechanisms for data transmitted over a communications network, Communications/network controls with supporting implementation features; Integrity controls; Message authentication; Access controls;

Encryption; Alarm; Audit trails; Entity authentication; and Event reporting.

In this final rule, we consolidate these provisions into § 164.312. That section now includes standards regarding access controls, audit controls, integrity (previously titled data authentication), person or entity authentication, and transmission security. As discussed below, while certain implementation specifications are required, many of the proposed security implementation features are now addressable implementation specifications. The function of authorization control has been incorporated into the information access management standard under § 164.308, Administrative safeguards.

1. Access Control (§ 164.312(a)(1))

In the proposed rule, we proposed to require that the access controls requirement include features for emergency access procedures and provisions for context-based, role-based, and/or user-based access; we also proposed the optional use of encryption as a means of providing access control. In this final rule, we require unique user identification and provision for emergency access procedures, and retain encryption as an addressable implementation specification. We also make ''Automatic logoff'' an addressable implementation specification. ''Automatic logoff'' and ''Unique user identification'' were formerly implementation features under the proposed ''Entity authentication'' (see § 164.312(d)).

a. *Comment:* Some commenters believe that in specifying ''Context,'' ''Role,'' and ''User'' based controls, use of other controls would effectively be excluded, for example, ''Partition rule-based access controls,'' and the development of new access control technology.

Response: We agree with the commenters that other types of access controls should be allowed. There was no intent to limit the implementation features to the named technologies and this final rule has been reworded to make it clear that use of any appropriate access control mechanism is allowed. Proposed implementation features titled ''Context-based access,'' ''Role-based access,'' and ''User-based access'' have been deleted and the access control standard at § 164.312(a)(1) states the general requirement.

b. *Comment:* A large number of comments were received objecting to the identification of ''Automatic logoff'' as a mandatory implementation feature. Generally the comments asked that we not be so specific and allow other forms of inactivity lockout, and that this type of feature be made optional, based more on the particular configuration in use and a risk assessment/analysis.

Response: We agree with the comments that mandating an automatic logoff is too specific. This final rule has been written to clarify that the proposed implementation feature of automatic logoff now appears as an addressable access control implementation specification and also permits the use of an equivalent measure.

c. *Comment:* We received comments asking that encryption be deleted as an implementation feature and stating that encryption is not required for ''data at rest.''

Response: The use of file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, which is a form of control. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity's risk analysis. Therefore, encryption has been adopted as an addressable implementation specification in this final rule.

d. *Comment:* We received one comment stating that the proposed implementation feature ''Procedure for emergency access,'' is not access control and recommending that emergency access be made a separate requirement.

Response: We believe that emergency access is a necessary part of access controls and, therefore, is properly a required implementation specification of the ''Access controls'' standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.

2. Audit Controls (§ 164.312(b))

We proposed that audit control mechanisms be put in place to record and examine system activity. We adopt this requirement in this final rule.

a. *Comment:* We received a comment stating that ''Audit controls'' should be an implementation feature rather than the standard, and suggesting that we change the title of the standard to ''Accountability,'' and provide additional detail to the audit control implementation feature.

Response: We do not adopt the term ''Accountability'' in this final rule because it is not descriptive of the requirement, which is to have the capability to record and examine system activity. We believe that it is appropriate to specify audit controls as a type of technical safeguard. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses. For example, see NIST Special Publication 800–14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* and NIST Special Publication 800–33, *Underlying Technical Models for Information Technology Security*.

b. *Comment:* One commenter recommended that this final rule state that audit control mechanisms should be implemented based on the findings of an entity's risk assessment and risk analysis. The commenter asserted that audit control mechanisms should be utilized only when appropriate and necessary and should not adversely affect system performance.

Response: We support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be. We believe that the audit control requirement should remain mandatory, however, since it provides a means to assess activities regarding the electronic protected health information in an entity's care.

c. *Comment:* One commenter was concerned about the interplay of State and Federal requirements for auditing of privacy data and requested additional guidance on the interplay of privacy rights, laws, and the expectation for audits under the rule.

Response: In general, the security standards will supercede any contrary provision of State law. Security standards in this final rule establish a minimum level of security that covered entities must meet. We note that covered entities may be required by other Federal law to adhere to additional, or more stringent security measures. Section 1178(a)(2) of the statute provides several exceptions to this general rule. With regard to protected health information, the preemption of State laws and the relationship of the Privacy Rule to other Federal laws is discussed in the Privacy Rule beginning at 65 FR 82480; the preemption provisions of the rule are set out at 45 CFR part 160, subpart B.

It should be noted that although the Privacy Rule does not incorporate a requirement for an ''audit trail'' function, it does call for providing an accounting of certain disclosures of protected health information to an

individual upon request. There has been a tendency to assume that this Privacy Rule requirement would be satisfied via some sort of process involving audit trails. We caution against assuming that the Security Rule's requirement for an audit capability will satisfy the Privacy Rule's requirement regarding accounting for disclosures of protected health information. The two rules cover overlapping, but not identical information. Further, audit trails are typically used to record uses within an electronic information system, while the Privacy Rule requirement for accounting applies to certain disclosures outside of the covered entity (for example, to public health authorities).

3. Integrity (§ 164.312(c)(1))

We proposed under the ''Data authentication'' requirement, that each organization be required to corroborate that data in its possession have not been altered or destroyed in an unauthorized manner and provided examples of mechanisms that could be used to accomplish this task. We adopt the proposed requirement for data authentication in the final rule as an addressable implementation specification ''Mechanism to authenticate data,'' under the ''Integrity'' standard.

a. *Comment:* We received a large number of comments requesting clarification of the ''Data authentication'' requirement. Many of these comments suggested that the requirement be called ''Data integrity'' instead of ''Data authentication.'' Others asked for guidance regarding just what ''data'' must be authenticated. A significant number of commenters indicated that this requirement would put an extraordinary burden on large segments of the health care industry, particularly when legacy systems are in use. Requests were received to make this an ''optional'' requirement, based on an entity's risk assessment and analysis.

Response: We adopt the suggested ''integrity'' terminology because it more clearly describes the intent of the standard. We retain the meaning of the term ''Data authentication'' under the addressable implementation specification ''Mechanism to authenticate data,'' and provide an example of a potential means to achieve data integrity.

Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanisms that are ubiquitous in hardware and operating systems today. The risk analysis process will address what data must be authenticated and should provide answers appropriate to the different situations faced by the various health care entities implementing this regulation.

Further, we believe that this standard will not prove difficult to implement, since there are numerous techniques available, such as processes that employ digital signature or check sum technology to accomplish the task.

b. *Comment:* We received numerous comments suggesting that ''Double keying'' be deleted as a viable ''Data authentication'' mechanism, since this practice was generally associated with the use of punched cards.

Response: We agree that the process of ''Double keying'' is outdated. This final rule omits any reference to ''Double keying.''

4. Person or Entity Authentication (§ 164.312(d))

We proposed that an organization implement the requirement for ''Entity authentication'', the corroboration that an entity is who it claims to be. ''Automatic logoff'' and ''Unique user identification'' were specified as mandatory features, and were to be coupled with at least one of the following features: (1) A ''biometric'' identification system; (2) a ''password'' system; (3) a ''personal identification number''; and (4) ''telephone callback,'' or a ''token'' system that uses a physical device for user identification.

In this final rule, we provide a general requirement for person or entity authentication without the specifics of the proposed rule.

Comment: We received comments from a number of organizations requesting that the implementation features for entity authentication be either deleted in their entirety or at least be made optional. On the other hand, comments were received requesting that the use of digital signatures and soft tokens be added to the list of implementation features.

Response: We agree with the commenters that many different mechanisms may be used to authenticate entities, and this final rule now reflects this fact by not incorporating a list of implementation specifications, in order to allow covered entities to use whatever is reasonable and appropriate. ''Digital signatures'' and ''soft tokens'' may be used, as well as many other mechanisms, to implement this standard.

The proposed mandatory implementation feature, ''Unique user identification,'' has been moved from this standard and is now a required implementation specification under ''Access control'' at § 164.312(a)(1). ''Automatic logoff'' has also been moved from this standard to the ''Access control'' standard and is now an addressable implementation specification.

5. Transmission Security (§ 164.312(e)(1))

Under ''Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted Over a Communications Network,'' we proposed that ''Communications/network controls'' be required to protect the security of health information when being transmitted electronically from one point to another over open networks, along with a combination of mandatory and optional implementation features. We proposed that some form of encryption must be employed on ''open'' networks such as the Internet or dial-up lines.

In this final rule, we adopt integrity controls and encryption, as addressable implementation specifications.

a. *Comment:* We received a number of comments asking for overall clarification as well as a definition of terms used in this section. A definition for the term ''open networks'' was the most requested action, but there was a general expression of dislike for the manner in which we approached this section, with some comments suggesting that the entire section be rewritten. A significant number of comments were received on the question of encryption requirements when dial-up lines were to be employed as a means of connectivity. The overwhelming majority strongly urged that encryption not be mandatory when using any transmission media other than the Internet, but rather be considered optional based on individual entity risk assessment/analysis. Many comments noted that there are very few known breaches of security over dial-up lines and that nonjudicious use of encryption can adversely affect processing times and become both financially and technically burdensome. Only one commenter suggested that ''most'' external traffic should be encrypted.

Response: In general, we agree with the commenters who asked for clarification and revision. This final rule has been significantly revised to reflect a much simpler and more direct requirement. The term ''Communications/network controls'' has been replaced with ''Transmission security'' to better reflect the requirement that, when electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk.

We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very small probability of interception.

Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet.

As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

We do not use the term ''open network'' in this final rule because its meaning is too broad. We include as an addressable implementation specification the requirement that transmissions be encrypted when appropriate based on the entity's risk analysis.

b. *Comment:* We received comments requesting that the implementation features be deleted or made optional. Three commenters asked that the requirement for an alarm be deleted.

Response: This final rule has been revised to reflect deletion of the following implementation features: (1) The alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for ''Communications/network controls'' and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features. ''Access controls'' has also been deleted from the implementation features since the consideration of the use of encryption will satisfy the intent of this feature. We retain as addressable implementation specifications two features: (1) ''Integrity controls'' and ''encryption''. ''Message authentication'' has been deleted as an implementation feature because the use of data authentication codes (called for in the ''integrity controls'' implementation specification) satisfies the intent of ''Message authentication.''

c. *Comment:* A number of comments were received asking that this final rule establish a specific (or at least a minimum) cryptographic algorithm strength. Others recommended that the rule not specify an encryption strength since technology is changing so rapidly. Several commenters requested guidelines and minimum encryption standards for the Internet. Another stated that, since an example was included (small or rural providers for example), the government should feel free to name a specific encryption package. One commenter stated that the requirement for encryption on the Internet should reference the ''CMS Internet Security Policy.''

Response: We remain committed to the principle of technology neutrality and agree with the comment that rapidly changing technology makes it impractical and inappropriate to name a specific technology. Consistent with this principle, specification of an algorithm strength or specific products would be inappropriate. Moreover, rapid advances in the success of ''brute force'' cryptanalysis techniques suggest that any minimum specification would soon be outmoded. We maintain that it is much more appropriate for this final rule to state a general requirement for encryption protection when necessary and depend on covered entities to specify technical details, such as algorithm types and strength. Because ''CMS Internet Security Policy'' is the policy of a single organization and applies only to information sent to CMS, and not between all covered entities, we have not referred to it here.

d. *Comment:* The proposed definition of ''Integrity controls'' generated comments that asked that the word ''validity'' be changed to ''Integrity.'' Commenters were concerned about the ability of an entity to ensure that information was ''valid.''

Response: We agree with the commenters about the meaning of the word ''validity'' in the context of the proposed definition of ''Integrity controls.'' We have named ''integrity controls'' as an implementation specification in this final rule to require mechanisms to ensure that electronically transmitted information is not improperly modified without detection (see § 164.312(c)(1)).

e. *Comment:* Three commenters asked for clarification and guidance regarding the unsolicited electronic receipt of health information in an unsecured manner, for example, when the information was submitted by a patient via e-mail over the Internet. Commenters asked for guidance as to what was their obligation to protect data received in this manner.

Response: The manner in which electronic protected health information is received by a covered entity does not affect the requirement that security protection must subsequently be afforded to that information by the covered entity once that information is in possession of the covered entity.

6. Proposed Requirements Not Adopted in This Final Rule

a. *Authorization Control*

We proposed, under ''Technical Security Services to Guard Data Integrity, Confidentiality, and Availability,'' that a mechanism be required for obtaining consent for the use and disclosure of health information using either ''Role-based access'' or ''User-based access'' controls. In this final rule, we do not adopt this requirement.

Comment: We received a large number of comments regarding use of the word ''consent.'' It was pointed out that this could be construed to mean patient consent to the use or disclosure of patient information, which would make this a privacy issue, rather than one of security. Other comments suggested deletion of the requirement in its entirety. We received a comment asking for clarification about the distinction between ''Access control'' and ''Authorizations.''

Response: These requirements were intended to address authorization of workforce members and others for the use and disclosure of health information, not patient consent. Upon reviewing the differences between ''Access control'' and ''Authorization control,'' we found it to be unnecessary to retain ''Authorization control'' as a separate requirement. Both the access control and the authorization control proposed requirements involved implementation of types of automated access controls, that is, role-based access and user-based access. It can be argued that the process of managing access involves allowing and restricting access to those individuals that have been authorized to access the data. The intent of the proposed authorization control implementation feature is now

incorporated in the access authorization implementation specification under the information access management standard in § 164.308(a)(4). Under the information access management standard, a covered entity must implement, if appropriate and reasonable to its situation, policies and procedures first to authorize a person to access electronic protected health information and then to actually establish such access. These policies and procedures will enable entities to follow the Privacy Rule minimum necessary requirements, which provide when persons should have access to information.

H. Organizational Requirements (§ 164.314)

We proposed that each health care clearinghouse must comply with the security standards to ensure all health information and activities are protected from unauthorized access. If the clearinghouse is part of a larger organization, then unauthorized access by the larger organization must be prevented. We also proposed that parties processing data through a third party would be required to enter into a chain of trust partner agreement, a contract in which the parties agree to electronically exchange data and to protect the transmitted data in accordance with the security standards.

In this final rule, we have adopted the concepts of hybrid and affiliated entities, as previously defined in § 164.504, and now defined in § 164.103, and business associates as defined in § 160.103, to be consistent with the Privacy Rule. General organizational requirements related to affiliated covered entities and hybrid entities are now contained in a new § 164.105. The proposed chain of trust partner agreement has been replaced by the standards for business associate contracts or other arrangements and the standards for group health plans. Consistent with the statute and the policy of the Privacy Rule, this final rule does not require noncovered entities to comply with the security standards.

1. Health Care Clearinghouses

The proposed rule proposed that if a health care clearinghouse were part of a larger organization, it would be required to ensure that all health information pertaining to an individual is protected from unauthorized access by the larger organization; this statement closely tracked the statutory language in section 1173(d)(1)(B) of the Act. Since the point of the statutory language is to ensure that health care information in the possession of a health care clearinghouse is not inappropriately accessed by the larger organization of which it is a part, this final rule implements the statutory language through the information access management provision of § 164.308(a)(4)(ii)(A).

The final rule, at § 164.105, makes the health care component and affiliated entity standards of the Privacy Rule applicable to the security standards. Therefore, we have not changed those standards substantively. In pertaining to the Privacy Rule, we have simply moved them to a new location in part 164. Any differences between § 164.105 and § 164.504(a) through (d) reflects the addition of requirements specific to the security standards.

The health care component approach was developed in response to extensive comment received principally on the Privacy Rule. See 65 FR 82502 through 82503 and 82637 through 82640 for a discussion of the policy concerns underlying the health care component approach. Since the security standards are intended to support the protection of electronic information protected by the Privacy Rule, it makes sense to incorporate organizational requirements that parallel those required of covered entities by the Privacy Rule. This policy will also minimize the burden of complying with both rules.

a. *Comment:* Relative to the following preamble statement (63 FR 43258): ''If the clearinghouse is part of a larger organization, then security must be imposed to prevent unauthorized access by the larger organization.'' One commenter asked what is considered to be ''the larger organization.'' For example, if a clearinghouse function occurs in a department of a larger business entity, will the regulation cover all internal electronic communication, such as e-mail, within the larger business and all external electronic communication, such as e-mail with its owners?

Response: The ''larger organization'' is the overall business entity that a clearinghouse would be part of. Under the Security Rule, the larger organization must assure that the health care clearinghouse function has instituted measures to ensure only that electronic protected health information that it processes is not improperly accessed by unauthorized persons or other entities, including the larger organization. Internal electronic communication within the larger organization will not be covered by the rule if it does not involve the clearinghouse, assuming that it has designated health care components, of which the health care clearinghouse is one. External communication must be protected as sent by the clearinghouse, but need not be protected once received.

b. *Comment:* One commenter asked that the first sentence in § 142.306(b) of the proposed rule, ''If a health care clearinghouse is part of a larger organization, it must assure all health information is protected from unauthorized access by the larger organization'' be expanded to read, ''If a health care clearinghouse or any other health care entity is part of a larger organization . . .''

Response: The Act specifically provides, at section 1173(d)(1)(B), that the Secretary must adopt standards to ensure that a health care clearinghouse, if part of a larger organization, has policies and security procedures to protect information from unauthorized access by the larger organization.

Health care providers and health plans are often part of larger organizations that are not themselves health care providers or health plans. The security measures implemented by health plans and covered health care providers should protect electronic protected health information in circumstances such as the one identified by the commenter. Therefore, we agree with the comment that the requirement should be expanded as suggested by the commenter. In this final rule, those components of a hybrid entity that are designated as health care components must comply with the security standards and protect against unauthorized access with respect to the other components of the larger entity in the same way as they must deal with separate entities.

2. Business Associate Contracts and Other Arrangements

We proposed that parties processing data through a third party would be required to enter into a chain of trust partner agreement, a contract in which the parties agree to electronically exchange data and to protect the transmitted data. This final rule narrows the scope of agreements required. It essentially tracks the provisions in § 164.502(e) and § 164.504(e) of the Privacy Rule, although appropriate modifications have been made in this rule to the required elements of the contract.

In this final rule, a contract between a covered entity and a business associate must provide that the business associate must—(1) implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates,

receives, maintains, or transmits on behalf of the covered entity; (2) ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards; (3) report to the covered entity any security incident of which it becomes aware; (4) make its policies and procedures, and documentation required by this subpart relating to such safeguards, available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and (5) authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

When a covered entity and its business associate are both governmental entities, an ''other arrangement'' is sufficient. The covered entity is in compliance with this standard if it enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of the above-described business associate contract. However, the covered entity may omit from this memorandum the termination authorization required by the business associate contract provisions if this authorization is inconsistent with the statutory obligations of the covered entity or its business associate. If other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of the above-described business associate contract, a contract or agreement is not required. If a covered entity enters into other arrangements with another governmental entity that is a business associate, such arrangements may omit provisions equivalent to the termination authorization required by the business associate contract, if inconsistent with the statutory obligation of the covered entity or its business associate.

If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to receive, create, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of the above-described business associate contract, *provided that* the covered entity attempts in good faith to obtain satisfactory assurances as required by the above described business associate contract and documents the attempt and the reasons that these assurances cannot be obtained.

We have added a standard for group health plans that parallels the provisions of the Privacy Rule. It became apparent during the course of the security and privacy rulemaking that our original chain of trust approach was both overly broad in scope and failed to address appropriately the circumstances of certain covered entities, particularly the ERISA group health plans. These latter considerations and the solutions arrived at in the Privacy Rule are described in detail in the Privacy Rule at 65 FR 82507 through 82509. Because the purpose of the security standards is in part to reinforce privacy protections, it makes sense to align the organizational policies of the two rules. This decision should also make compliance less burdensome for covered entities than would a decision to have different organizational requirements for the two sets of rules.

Thus, we have added at § 164.314(b) a standard for group health plan that tracks the standard at § 164.504(f) very closely. The purpose of these provisions is to ensure that, except when the electronic protected health information disclosed to a plan sponsor is summary health information or enrollment or disenrollment information as provided for by § 164.504(f), group health plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan. The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; ensure that any agents, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards to protect the information; report to the group health plan any security incident of which it becomes aware; and make its policies and procedures and documentation relating to these safeguards available to the Secretary for purposes of determining the group health plan's compliance with this subpart.

a. *Comment:* Several commenters expressed confusion concerning the applicability of proposed § 142.104 to security.

Response: The proposed preamble included language generally applicable to most of the proposed standards under HIPAA. Proposed § 142.104 concerned general requirements for health plans relative to processing transactions. We proposed that plans could not refuse to conduct a transaction as a standard transaction, or delay or otherwise adversely affect a transaction on the grounds that it was a standard transaction; health information transmitted and received in connection with a transaction must be in the form of standard data elements; and plans conducting transactions through an agent must ensure that the agent met all the requirements that applied to the health plan. Except for the statement that a plan's agent (''business associate'' in the final rule) must meet the requirements (which would include security) that apply to the health plan, this proposed section did not pertain to the security standards and was addressed in the Transaction Rule.

b. *Comment:* The majority of comments concerned proposed rule language stating ''the same level of security will be maintained at all links in the chain * * *'' Commenters believed the current language will have an adverse impact on one of the security standard's basic premises, which is scalability. It was requested that the language be changed to indicate that, while appropriate security must be maintained, all partners do not need to maintain the same level of security.

A number of commenters expressed some confusion concerning their responsibility for the security of information once it has passed from their control to their trading partner's control, and so on down the trading partner chain. Requests were made that we clarify that chain of trust partner agreements were really between two parties, and that, if a trading partner agreement has been entered into, any given partner would not be responsible, or liable, for the security of data once it is out of his or her control.

In line with this concern, several commenters were concerned that they would have some responsibility to ensure the level of security maintained by their trading partner.

Several commenters believe a chain of trust partner agreement should not be a security requirement. One commenter stated that because covered entities must already conform to the regulation

requirements, a ''chain of trust'' agreement does not add to overall security. Compliance with the regulation should be sufficient.

Response: We believe the commenters are correct that the rule as proposed would—(1) not allow for scalability; and (2) would lead an entity to believe it is responsible, and liable, for making sure all entities down the line maintain the same level of security. The confusion here seems to come from the phrase ''same level of security.'' Our intention was that each trading partner would maintain reasonable and appropriate safeguards to protect the information. We did not mean that partners would need to implement the same security technology or measures and procedures.

We have replaced the proposed ''Chain of trust'' standard with a standard for ''Business associate contracts and other arrangements.''

When another entity is acting as a business associate of a covered entity, we require the covered entity to require the other entity to protect the electronic protected health information that it creates, receives, maintains or transmits on the covered entity's behalf. The level of security afforded particular electronic protected health information should not decrease just because the covered entity has made the business decision to entrust a business associate with using or disclosing that information in connection with the performance of certain functions instead of doing those functions itself. Thus, the rule below requires covered entities to require their business associates to implement certain safeguards and take other measures to ensure that the information is safeguarded (see § 164.308(b)(1) and § 164.314(a)(1)).

The specific requirements of § 164.314(a)(1) are drawn from the analogous requirements at 45 CFR 164.504(e) of the Privacy Rule, although they have been adapted to reflect the objectives and context of the security standards. Compare, in particular, 45 CFR 164.504(e)(2)(ii) with § 164.314(a)(1). We have not imported all of the requirements of 45 CFR 164.504(e), however, as many have no clear analog in the security context (see, for example, 45 CFR 164.504(e)(2)(i) regarding permitted and required uses and disclosures made by a business associate). HHS had previously committed to reconciling its security and privacy policies regarding business associates (see 65 FR 82643). The close relationship of many of the organizational requirements in section 164.314 with the analogous requirements of the Privacy Rule should facilitate the implementation and coordination of security and privacy policies and procedures by covered entities.

In contrast, when another entity is not acting as a business associate for the covered entity, but rather is acting in the capacity of some other sort of trading partner, we do not require the covered entity to require the other entity to adopt particular security measures, as previously proposed. This policy is likewise consistent with the general approach of the Privacy Rule (see the discussion in the Privacy Rule at 65 FR 82476). The covered entity is free to negotiate security arrangements with its non-business associate trading partners, but this rule does not require it to do so.

A similar approach underlies § 164.314(b) below. These provisions are likewise drawn from, and intended to support, the analogous privacy protections provided for by 45 CFR 164.504(f) (see the discussion of § 164.504(f) of the Privacy Rule at 65 FR 82507 through 82509, and 82646 through 82648). As with the business associate contract provisions, however, they are imported and adapted only to the extent they make sense in the security context. Thus, for example, the requirement at § 164.504(f)(2)(ii)(C) prohibits the plan documents from permitting disclosure of protected health information to the plan sponsor for employment-related purposes. As this prohibition goes entirely to the permissibility of a particular type of disclosure, it has no analog in § 164.314(b).

c. *Comment:* Several commenters stated that if security features are determined by agreements established between ''trading partners,'' as stated in the proposed regulations, there should be some guidelines or boundaries for those agreements so that extreme or unusual provisions are not permitted.

Response: This final rule sets a baseline, or minimum level, of security measures that must be taken by a covered entity and stipulates that a business associate must also implement reasonable and appropriate safeguards. This final rule does not, however, prohibit a covered entity from employing more stringent security measures or from requiring a business associate to employ more stringent security measures. A covered entity may determine that, in order to do business with it, a business associate must also employ equivalent measures. This would be a business decision and would not be governed by the provisions of this rule. Security mechanisms relative to the transmission of electronic protected health information between entities may need to be agreed upon by both parties in order to successfully complete the transmission. However, the determination of the specific transmission mechanisms and the specific security features to be implemented remains a business decision.

d. *Comment:* Several commenters asked whether existing contracts could be used to meet the requirement for a trading partner agreement, or does the rule require entry into a new contract specific to this purpose. Also, the commenters want to know about those whose working agreements do not involve written contractual agreement: Do they now need to set up formal agreements and incur the additional expense that would entail?

Response: This final rule requires written agreements between covered entities and business associates. New contracts do not have to be entered into specifically for this purpose, if existing written contracts adequately address the applicable requirements (or can be amended to do so).

e. *Comment:* Several commenters asked whether covered entities are responsible for the security of all individual health information sent to them, or only information sent by chain of trust partners. They also asked if they can refuse to process standard transactions sent to them in an unsecured fashion. In addition, they inquired if they can refuse to send secured information in standard transactions to entities not required by law to secure the information. One commenter asked if there is a formula for understanding in any particular set of relationships where the ultimate responsibility for compliance with the standards would lie.

Response: Pursuant to the Transactions Rule, if a health plan receives an unsecured standard transaction, it may not refuse to process that transaction simply because it was sent in an unsecured manner. The health plan is not responsible under this rule, for how the transaction was sent to it (unless the transmission was made by a business associate, in which case different considerations apply); however, once electronic protected health information is in the possession of a covered entity, the covered entity is responsible for the security of the electronic protected health information received. The covered entity must implement technical security mechanisms to guard against unauthorized access to electronic protected health information that is transmitted over an electronic communication network. In addition, the rule requires the transmitting

covered entity to obtain written assurance from a business associate receiving the transmission that it will provide an adequate level of protection to the information. For the business associate provisions, see § 164.308(b) and § 164.314(a) of this final rule.

f. *Comment:* One commenter asked what security standards a vendor having access to a covered entity's health information during development, testing, and repair must meet and wanted to know whether the rule anticipates having a double layer of security compliance (one at the user level and one at the vendor level). If so, the commenter believes this will cause duplication of work.

Response: In the situation described, the vendor would be acting as a business associate. The covered entity must require the business associate to implement reasonable and appropriate security protections of electronic protected health information. This requirement, however, does not impose detailed requirements for how that level of protection must be achieved. The resulting flexibility should permit entities and their business associates to adapt their security safeguards in ways that make sense in their particular environments.

g. *Comment:* A number of commenters requested sample contract language or models of contracts. We also received one comment that suggested that we should not dictate the contents of contracted agreements.

Response: We will consider developing sample contract language as part of our guideline development.

I. Policies and Procedures and Documentation Requirements (§ 164.316)

We proposed requiring documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. We proposed that the documentation be reviewed and updated periodically.

We have emphasized throughout this final rule the scalability allowed by the security standards. This final rule requires covered entities to implement policies and procedures that are reasonably designed, taking into account the size and type of activities of the covered entity that relate to electronic protected health information, and requires that the policies and procedures must be documented in written form, which may be in electronic form. This final rule also provides that a covered entity may change its policies and procedures at any time, provided that it documents and implements the changes in accordance with the applicable requirements. Covered entities must also document designations, for example, of affiliation between covered entities (see § 164.105(b)), and other actions, as required by other provisions of the subpart.

1. *Comment:* One commenter wanted development of written policies regarding such things as confidentiality and privacy rights for access to medical records, and approval of research by a review board when appropriate.

Response: These issues are covered in the Privacy Rule (65 FR 82462) (see, in particular, § 164.512(i), § 164.524, and § 164.530(i)).

2. *Comment:* One commenter asked if standards will override agreements that require others to maintain hardcopy documentation (for example, signature on file) and no longer require submitters to maintain hardcopy documentation.

Response: The security standards will require a minimum level of documentation of security practices. Any agreements between trading partners for the exchange of electronic protected health information that impose additional documentation requirements will not be overridden by this final rule.

3. *Comment:* One commenter stated that there should be a requirement to document only applications deemed necessary by an applications and data criticality assessment.

Response: Electronic protected health information must be afforded security protection under this rule regardless of what application it resides in. The measures taken to protect that information must be documented.

4. *Comment:* One commenter asked how detailed the documentation must be. Another commenter asked what ''kept current'' meant.

Response: Documentation must be detailed enough to communicate the security measures taken and to facilitate periodic evaluations pursuant to § 164.308(a)(8). While the term ''current'' is not in the final rule, this concept has been adopted in the requirement that documentation must be updated as needed to reflect security measures currently in effect.

5. *Comment:* We received one comment concerning review and updating of implementing documentation suggesting that ''periodically'' be changed to ''at least annually.''

Response: We believe that the requirement should remain as written, in order to allow individual entities to establish review and update cycles as deemed necessary. The need for review and update will vary dependent upon a given entity's size, configuration, environment, operational changes, and the security measures implemented.

J. Compliance Dates for Initial Implementation (§ 164.318)

We proposed that how the security standard would be implemented by each covered entity would be dependent upon industry trading partner agreements for electronic transmissions. Covered entities would be able to adapt the security matrix to meet business needs. We suggested that requirements of the security standard may be implemented earlier than the compliance date. However, we would require implementation to be complete by the applicable compliance date, which is 24 months after adoption of the standard, and 36 months after adoption of the standard for small health plans, as provided by the Act. In the proposed rule, we suggested that an entity choosing to convert from paper to standard EDI transactions, before the effective date of the security standard, consider implementing the security standard at the same time.

In this final rule the dates by which entities must be in compliance with the standards are called ''compliance dates,'' consistent with our practice in the Transactions, Privacy, and Employer Identifier Rules. Section 164.318 in this final rule is also organized consistent with the format of those rules. The substantive requirements, which are statutory, remain unchanged.

Many of the comments received concerning effective dates and compliance dates, including the compliance dates for modifications of standards, were addressed in the Transactions Rule. Those that were not addressed in that publication are presented below.

1. *Comment:* A number of commenters expressed support for the effective dates of the rules and stated that they should not be delayed. In contrast, one commenter stated that we should delay this rule to allow for an open consensus building debate to occur concerning security. One commenter asked that the rule be delayed until after implementation of the ICD-CM changes.

A number of comments were received expressing the opinion that the security regulation should not be published until either the Congress has enacted legislation governing standards with respect to the privacy of individually identifiable health information, or the Secretary of HHS has promulgated final regulations containing these standards. One commenter stated, ''we find

ourselves in the difficult position of reacting to proposed rules setting the standards for how information should be physically and electronically protected, without having reached agreement on the larger issues of consent for and disclosure of individual medical information.''

Response: The effective date of the final rule is 60 days after this final rule is published in the **Federal Register**. The statute sets forth the compliance dates for the standards. Covered entities must comply with this final rule no later than 24 months (36 months for small plans) after the effective date.

The final Privacy Rule has already been published. We note that numerous comments concerning the timing of the adoption of privacy and security standards were also received in the privacy rulemaking and are discussed in the Privacy Rule at 65 FR 82752.

2. *Comment:* One commenter asked that proposed § 142.312 be rewritten to separate the effective dates for the Security Rule and the Transactions Rule.

Response: The proposed rule incorporated general language applicable to all the proposed Administrative Simplification standards. Language concerning standards other than Security is not included in § 164.318. Because this final rule is adopted after the Transactions Rule was adopted, the compliance dates for the security standards differ from those for the transactions standards. Comments concerning general effective dates were addressed in the Transactions Rule. Comments specific to the security standards are addressed here.

3. *Comment:* Several commenters suggested that we not allow early implementation of the Security Rules. A number of others asked that we allow, but not require, early implementation by willing trading partners. Another commenter suggested that early implementation by willing trading partners be allowed as long as the data content transmitted is equal to that required by statute. Another commenter requested that it be stipulated that entities cannot implement less than 1 year from the date of this final rule and then only after successful testing, and that a ''start testing by'' date be defined.

Response: Whether or not to implement before the compliance date is a business decision that each covered entity must make. Moreover, the vast majority of the standards address internal policies and procedures that can be implemented at any time without any impact on trading partners.

4. *Comment:* One commenter asked us to establish a research site or test laboratory for a trial implementation.

Response: The concept of a ''trial implementation'' that would have widespread relevance is inconsistent with our basic principles of flexibility, scalability, and technology-neutrality.

5. *Comment:* One commenter stated that the 2-year time frame for implementation of a contingency plan is too short for health plans that serve multiple regions of the country.

Response: The Congress mandated that entities must be in compliance 2 years from the initial standard's adoption date (3 years for small plans).

K. Appendix

The proposed rule contained three addenda. Addendum 1 set out in matrix form the proposed requirements and related implementation features of the proposed rule. Addendum 2 set out in list form a glossary of terms with citations to the sources of those terms. Addendum 3 identified and mapped areas of overlap in the proposed security standard and implementation features.

This final rule retains only the first proposed addendum, the matrix, as an appendix, that is modified to reflect the changes in the administrative, physical, and technical safeguard portions of the rule below. Numerous terms in the glossary now appear in the rule below, typically (but not always) as definitions.

1. *Comment:* Over two-thirds of the comments received on this topic asked that the matrix be incorporated into the final rule. One commenter asked that a simplified version be made part of the final rule. Six commenters wanted it kept in this final rule as an addendum. One commenter stated that it should be in an appendix to the rule, while others stated that it should not be included in this final rule.

Response: Since a significant majority of commenters requested retention of the matrix, it has been incorporated into this final rule as an appendix. The matrix displays, in tabular form, the administrative, physical, and technical safeguard standards and relating implementation specifications described in this final rule in § 164.308, § 164.310, and § 164.312. It should be noted that the requirements of § 164.105, § 164.314, and § 164.316 are not presented in the matrix.

2. *Comment:* A large majority of commenters stated that the glossary located in Addendum 2 of the proposed rule should be included as part of the final rule. Several commenters asked that it be incorporated into the definitions section of the final rule. One commenter stated that the glossary should not be part of this final rule.

Response: The terms defined in the glossary in Addendum 2 of the proposed rule are found throughout this final rule, either as part of the text of § 164.306 through § 164.312 or under § 164.304, as appropriate. We included only terms relevant to the particular standards and implementation specifications being adopted.

3. *Comment:* Several commenters requested that the mapped matrix located in Addendum 3 of the proposed rule be included in this final rule, either as part of the rule or as an addendum, while others stated that it should not be part of this final rule. Several commenters cited items to be added to the mapped matrix.

Response: The mapped matrix was merely a snapshot of current standards and guidelines that the implementation team was able to obtain for review during the development of the security and electronic signature requirements and was provided in the proposed rule as background material. Since this matrix has not been fully populated or kept up-to-date, it is not being published as part of this final rule. Where relevant, we do reference various standards and guidelines indicated in the matrix in this preamble.

L. Miscellaneous Issues

1. Preemption

The statute requires generally that the security standards supersede contrary provisions of State law including State law requiring medical or health plan records to be maintained or transmitted in written rather than electronic formats. The statute provides certain exceptions to the general rule; section 1178(a)(2) of the Act identifies conditions under which an exception applies. The proposed rule did not provide for a process for making exception determinations; rather, a process was proposed in the privacy rulemaking and was adopted with the Privacy Rule (see part 160, subpart B). This process applies to exception determinations for all of the Administrative Simplification rules, including this rule.

a. *Comment:* Several commenters stated that the proposed rule does not include substantive protections for the privacy rights of patients' electronic medical records, while the rule attempts to preempt State privacy laws with respect to these records. Comments stated that, by omitting a clarification of State privacy law applicability, the proposed rule creates confusion. They believe that the rule must contain

express and specific exemptions of State laws with respect to medical privacy.

Response: The Privacy Rule establishes standards for the rights of patients in regard to the privacy of their medical records and for the allowable uses and disclosures of protected health information. The identified concerns were discussed in the Privacy Rule (see 65 FR 82587 through 82588). The security standards do not specifically address privacy but will safeguard electronic protected health information against unauthorized access or modification.

b. *Comment:* One commenter asked how these regulations relate to confidentiality laws, which vary from State to State.

Response: It is difficult to respond to this question in the abstract without the benefit of reference to a specific State statute. However, in general, these security standards will preempt contrary State laws. Per section 1178(a)(2) of the Act, this general rule would not hold if the Secretary determines that a contrary provision of State law is necessary for certain identified purposes to prevent fraud and abuse; to ensure appropriate State regulation of insurance and health plans; for State reporting on health care delivery costs; or if it addresses controlled substances. See 45 CFR part 160 subpart B. In such case, the contrary provision of State law would preempt a Federal provision of these security standards. State laws that are related but not contrary to this final rule, will not be affected.

Section 1178 of the Act also limits the preemptive effect of the Federal requirements on certain State laws other than where the Secretary makes certain determinations. Section 1178(b) of the Act provides that State laws for reporting of disease and other conditions and for public health surveillance, investigation, or intervention are not invalidated or limited by the Administrative Simplification rules. Section 1178(c) of the Act provides that the Federal requirements do not limit States' abilities to require that health plans report or provide access to certain information.

c. *Comment:* Several commenters stated that allowing State law to establish additional security restrictions conflicts with the purpose of the Federal rule and/or would make implementation very difficult. One commenter asked for clarification as to whether additional requirements tighter than the requirements outlined in the proposed rule may be imposed.

Response: The general rule is that the security standards in this final rule supersede contrary State law. Only where the Secretary has granted an exception under section 1178(a)(2)(A) of the Act, or in situations under section 1178(b) or (c) of the Act, will the general rule not hold true. Covered entities may be required to adhere to stricter State-imposed security measures that are not contrary to this final rule.

2. Enforcement

The proposed rule did not contain specific enforcement provisions. This final rule likewise does not contain specific enforcement provisions; it is expected that enforcement provisions applicable to all Administrative Simplification rules will be proposed in a future rulemaking.

a. *Comment:* One commenter voiced support for the proposed rule's approach. Another stated that the process is poorly defined. One commenter stated that fines should be eliminated, or the scope of activity subject to fines should be more narrowly defined.

While a number of commenters were of the opinion that HHS must retain enforcement responsibility, stating that it would be unconstitutional to give it to a private entity, several others stated that it may not be practical for HHS to retain the responsibility for determining violations and imposing penalties specified by the statute. A concern was voiced over HHS's ability to fairly and consistently apply the rules due to budget constraints. Several commenters support industry solutions to enforcement with some level of government involvement. One commenter recommended a single audit process using accrediting bodies already in place. Another stated that entities providing accreditation services should not be involved in enforcement as this would result in a conflict of interest.

Clarification was requested, including the use of examples, concerning what constitutes a violation, and how a penalty applies to a ''person.'' Commenters asked if the term ''person'' referred to the people responsible for the system and how penalties would apply to corporations and other entities.

Response: It is expected that enforcement of HIPAA standards will be addressed in regulations to be issued at a later date.

b. *Comment:* Several commenters stated that enforcement of the security standards will be arbitrarily delegated to private businesses that compete with physicians and with each other.

Response: These comments are premature for the reasons stated above.

3. Comment Period

The comment period on the proposed rule was 60 days.

Comment: We received comments suggesting that significant changes to the standards could occur in the final rule as a result of changes made in response to comments. The commenter believes such changes could adversely affect payers and providers, and suggested that the rule should be republished as a proposed rule with a new comment period to allow additional comments concerning any changes. A ''work-in-progress'' approach was also suggested, to give all stakeholders time to read, analyze, and comment upon evolving versions of a particular proposed rule.

Response: We have not accepted these suggestions. The numerous comments received were thoughtful, analytical, detailed, and addressed every area of the proposed rule. This response to the proposed rule indicates that the public had ample time to read, analyze, and comment upon the proposed rule. If we were to treat the rule as a ''work-in-progress'' and issue evolving versions, allowing for comments to each version, we would never implement the statute and achieve administrative simplification as directed by the Congress.

M. Proposed Impact Analysis

The preamble to the Transactions Rule contains comments and responses on the impact of all the administrative simplification standards in general except privacy. Comments and responses specific to the relative impact of implementing this final rule are presented below.

a. *Comment:* Several commenters stated that the proposed security standards are complex, costly, administratively burdensome, and could result in decreased use of EDI. One commenter stated that this rule runs counter to the explicit intent of Administrative Simplification that requires, ''any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.''

Several commenters expressed concern that there was no cost benefit analysis provided for these proposed regulations, stating that, faced with increasingly limited resources, it is essential that a security standards cost/benefit analysis for all health care trading partners be provided. Another said an independent cost estimate by the General Accounting Office (GAO) should be performed on these rules and

HHS cost estimates should be publicized for comparison purposes.

Still another commenter stated that HHS must provide accurate public sector implementation cost figures and provide funds to offset the cost burden.

One commenter asked for cost benefit evaluations to understand the relationship between competing technologies, levels of security and potential threats to be guarded against. These would demonstrate the costs and the benefits to be gained for both large and small organizations and would provide an understanding of how the levels of security vary by organization size and what the inducements and support available to facilitate adoption are. One commenter suggested that we establish a workgroup to more fully assess the costs and provide Federal funds to offset implementation costs.

One commenter noted a seeming disconnect between two statements in the preamble. Section A, Security standards, states, ''no individual small entity is expected to experience direct costs that exceed benefits as a result of this rule.'' In contrast, section E, Factors in establishing the security standards reads, ''We cannot estimate the per-entity cost of implementation because there is no information available regarding the extent to which providers', plans', and clearinghouses' current security practices are deficient.''

Response: We are unable to estimate, of the nation's 2 million-plus health plans and 1 million-plus providers that conduct electronic transactions, the number of entities that would require new or modified security safeguards and procedures beyond what they currently have in place. Nor are we able to estimate the number of entities that neither conduct electronic transactions nor maintain individually identifiable electronic health information but may become covered entities at some future time. As we are unable to estimate the number of entities and what measures are or are not already in place, or what specific implementation will be chosen to meet the requirements of the regulation, we are also unable to estimate the cost to those entities.

However, the use of electronic technology to maintain or transmit health information results in many new and potentially large risks. These risks represent expected costs, both monetary and social. Leaving risk assessment up to individual entities will minimize the impact and ensure that security effort is proportional to security risk.

As discussed earlier, the security requirements are both scalable and technically flexible. We have made significant changes to this final rule, reducing the number of required implementation features and providing for greater flexibility in satisfaction of the requirements. In other words, we have focused more on what needs to be done and less on how it should be accomplished.

We have removed the statement regarding the extent of costs versus benefits for small entities.

b. *Comment:* One commenter stated that on page 43262 of the proposed rule, it indicate that complexity of conversion to the security standards would be affected by the choice to use a clearinghouse. The commenter stated that this choice would have little effect on implementation of security standards. Another commenter stated that the complexity (and cost) of the conversion to meet the security standards is affected by far more than just the ''volume of claims health plans process electronically and the desire to transmit the claims or to use the services of a VAN or clearinghouse'' as is stated on page 43262. Because the security standards apply to internal systems as well as to transactions between entities, a number of additional factors must be considered, for example, modification of existing security mechanisms, legacy systems, architecture, and culture.

Response: We agree. We have modified the Regulatory Impact Analysis section to take into account that there are other factors involved, such as the architecture and technology limitations of existing systems.

c. *Comment:* One commenter stated that States will need 90 percent funding of development and implementation, without the burden of an advanced planning documents requirement, from us for this costly process to succeed. Any new operational obligation should be 100 percent funded. Also human resource obligations will be significant. Some States believe they will have difficulty obtaining the budget funds for the State share of the costs. State Medicaid agencies, as purchasers, may also face paying the implementation costs of health care providers, clearinghouses, and health plans in the form of higher rates.

Response: The statute does not authorize any new or special funding for implementation of the regulations. Medicaid system changes, simply because they are ''HIPAA related'' do not automatically qualify for 90 percent Federal funding participation. As with any systems request, the usual rules will be applied to determine funding eligibility for State HIPAA initiatives. Nevertheless, HHS recognizes that there are significant issues regarding the funding and implementation of HIPAA by Medicaid State agencies, and intends to address them through normal channels of communication with States.

d. *Comment:* One commenter stated that the proposed rule does not establish how the security standards will contribute to reduced cost for providers. One commenter expected the unintended result of this regulation will be impediment of EDI growth and perhaps even a decline in EDI use by providers. Another stated that the proposed rule actively discourages physician EDI participation by suggesting a fallback to paper processing for those unable to meet the cost of highly complex security compliance.

Response: Ensuring the integrity of an electronic message, its delivery to the correct person, and its confidentiality must be an integral part of conducting electronic commerce. We believe that the consistent application of the measures provided in this rule will actually encourage use of EDI because it will provide increased confidence in the reliability and confidentiality of health information to all parties involved. Also, the implementation of these security requirements will reduce the potential overall cost of risk to a greater extent than additional security controls will increase costs. Put another way, the potential cost of not reasonably addressing security risks could substantially exceed the cost of compliance.

e. *Comment:* One commenter stated that the implementation impact of the technical safeguards is clearly understated for physicians who use digitally-based equipment that has been in place for some time. The commenter believes that the rule will likely have greatest impact on the installed base of digital systems, including imaging modalities and other medical devices that store or transmit patient information because software for legacy systems will likely require retrofitting or replacement to come into compliance. The commenter believes that this is a negative impact and would outweigh any benefits derived from the potential risk of security breaches. The commenter recommended compliance for digital imaging devices be extended by an additional 3 years to allow time to upgrade systems and defray the associated costs.

Response: Compliance dates for the initial implementation of the initial standards are statutorily prescribed; therefore, we are unable to allow additional time outside of the statutory timeframes for compliance.

f. *Comment:* A commenter stated that, as a new regulatory mandate, HIPAA

costs must be factored into any base year calculations for the proposed prospective payment system. Without an adjustment, this will be another regulatory mandate that comes at the cost of patient care.

Response: Costs included in the prospective payment system are legislatively mandated. The Congress did not direct the inclusion of HIPAA costs into the system, so they are not included. However, the Department believes that the HIPAA standards will provide savings to the provider community over the next 10 years.

g. *Comment:* One commenter suggested that we include requirements for how a compliant business could dually operate—(1) in a HIPAA compliant manner; and (2) in their former noncompliant manner in order to accommodate doing business with other organizations that are not yet compliant.

Response: The statute imposes a 2-year implementation period between the adoption of the initial standards and the date by which covered entities (except small health plans) must be in compliance. An entity may come into compliance at any point in time during the 2 years. Therefore, the rule does not require a covered entity to comply before the established compliance date. Those entities that come into compliance before the 2-year deadline should decide how best to deal with entities that are not yet compliant. Further, we note that, generally speaking, compliance by a covered entity with these security rules will not hinge on compliance by other entities.

h. Comment: One commenter stated that privacy legislation could impose significant changes to written policies and procedures on authorization, access to health information, and how sensitive information is disclosed to others. The commenter believes these changes could mean the imposition of security requirements different from those contained in the proposed rule, and money spent complying with the security provisions could be ill spent if significant new requirements result from the privacy legislation.

Response: The privacy standards at subpart E of 42 CFR part 164 are now in effect, and this final rule is compatible with them. If, in the future, the Congress passes a law whose provisions differ from these standards, the standards would have to be modified.

i. Comment: One commenter stated that the private sector should develop educational tools or models in order to assist physicians, other providers, and health plans to comply with the security regulations.

Response: We agree. The health care industry is striving to do this. HHS is also considering provider outreach and education activities.

IV. Provisions of the Final Regulation

We have made the following changes to the provisions of the August 12, 1998 proposed rule. Specifically, we have—

- Changed the CFR part from 142 to 164.
- Removed information throughout the document pertaining to electronic signature standards. Electronic signature standards will be published in a separate final rule.
- Replaced the word ''requirement,'' when referring to a standard, with ''standard.'' Replaced ''Implementation feature'' with ''Implementation specification.''
- Made minor modifications to the text throughout the document for purposes of clarity.
- Modified numerous implementation features so that they are now addressable rather than mandatory.
- Removed the word ''formal'' when referring to documentation.
- Revised the phrase ''health information pertaining to an individual'' to ''electronic protected health information.''
- Added the following definitions to § 160.103: ''Disclosure,'' ''Electronic protected health information,'' ''Electronic media,'' ''Organized health care arrangement,'' and ''Use.''
- Removed proposed § 142.101 as this information is conveyed in § 160.101 and § 160.102 of the Privacy Rule (65 FR 82798). Removed proposed § 142.102 as it is redundant.
- Removed the following definitions from proposed § 142.103 since they are pertinent to other administrative simplification regulations and are defined elsewhere: code set, health care clearinghouse, health care provider, health information, health plan, medical care, small health plan, standard, and transaction.
- Moved the following definitions from § 164.501 to § 164.103 (proposed § 142.103): '' ''Plan sponsor'' and ''Protected health information.'' Added definitions of ''Covered functions'' and ''Required by law.''
- Removed proposed § 142.104, ''General requirements for health plans,'' and proposed § 142.105, ''Compliance using a health care clearinghouse,'' since these sections are not pertinent to the security standards.
- Removed proposed § 142.106, ''Effective dates of a modification to a standard or implementation specification,'' since this information is covered in the ''Standards for Electronic Transactions'' final rule (65 FR 50312).
- Moved proposed § 142.302 to § 164.302. Changed the section heading from ''Applicability and scope'' to ''Applicability.'' Modified language to state that covered entities must comply with the security standards.
- Moved proposed § 142.304 to § 164.304. Modified language to remove definitions of words and concepts not used in this final rule: ''Access control,'' ''Contingency plan,'' ''Participant,'' ''Role-based access control,'' ''Token,'' and ''User-based access.''
- Moved proposed § 142.304 to § 164.304. Modified language to add definitions requested by commenters; previously published in Addendum 2 but not in the draft regulation itself; or necessitated by the change of scope to electronic protected health information and alignment with the Privacy Rule to include: ''Administrative safeguards,'' ''Availability,'' ''Confidentiality,'' ''Data,'' ''Data authentication Code,'' ''Integrity,'' ''Electronic protected health information,'' ''Facility,'' ''Information System,'' ''Security or security measures,'' ''Security incident,'' ''Technical safeguards,'' ''User,'' and ''Workstation.''
- Moved definitions related to privacy from § 164.504 to new § 164.103: ''Common control,'' ''Common ownership,'' ''Health care component,'' ''Hybrid entity.''
- Moved proposed § 142.306, ''Rules for the security Standard,'' to § 164.306. Modified language to more clearly state the general requirements of the final rule relative to the standards and implementation specifications contained therein. Retitled the section as ''Security standards: General Rules.''
- Moved proposed § 142.308 to § 164.308. Where this section was proposed to contain all of the security standards in paragraphs (a) through (d), it now encompasses the Administrative safeguards.
- Moved and reorganized proposed § 142.308 (a) through (d) requirements to § 164.308, § 164.310, and § 164.312.
- Moved proposed § 142.308(a)(1), ''Certification,'' to § 164.308(a)(8). Modified language to indicate both technical and nontechnical evaluation is involved and renamed ''Evaluation''.
- Moved proposed § 142.308(a)(2), ''Chain of trust,'' to § 164.308(b)(1), renamed to ''Business associate contracts and other arrangements,'' and revised language to redefine who must enter into a contract under this rule for the protection of electronic protected health information.
- Moved proposed § 142.308(a)(3), ''Contingency plan,'' to

§ 164.308(a)(7)(i). Modified language to state that two implementation specifications, ''Applications and data criticality analysis'' and ''Testing and revision procedures,'' are addressable.

• Removed ''Formal mechanism for processing records'' (proposed § 142.308(a)(4)) since this requirement was determined to be in part intrusive into business functions and in part redundant.

• Moved proposed § 142.308(a)(5), ''Information access control,'' to § 164.308(a)(4)(i) and renamed as ''Information access management.'' Removed the word ''formal'' from description. Modified language to state that two implementation specifications (''Access Authorization'' and Access Establishment and Modification'') are addressable.

• Moved proposed § 142.308(a)(6), ''Internal audit,'' to § 164.308(a)(1)(ii)(D) as an implementation specification under the ''Security management process'' standard since this was determined to be a more logical placement of this item. Retitled, for clarity, ''Information system activity review.''

• Moved proposed § 142.308(a)(7), ''Personnel security,'' to § 164.308(a)(3)(i) and retitled ''Workforce security.'' Modified language to state that implementation specifications are addressable.

• Combined proposed § 142.308(a)(7)(i), and § 142.308(a)(7)(iii) (''Assuring supervision of maintenance personnel by an authorized, knowledgeable person'' and ''Assuring that operations and maintenance personnel have proper access authorization,'') under § 164.308(a)(3)(ii)(A) and renamed to ''Authorization and/or supervision.'' Modified description for clarity.

• Moved proposed § 142.308(a)(7)(iv), ''Personnel clearance procedure,'' to § 164.308(a)(3)(ii)(B), renamed to ''Workforce clearance procedure,'' and modified description for clarity.

• Removed proposed § 142.308(a)(7)(v), ''Personnel security policies and procedures,'' as this feature was determined to require redundant effort.

• Removed proposed § 142.308(a)(7)(vi), ''Security awareness training.'' Information concerning this subject has been incorporated under § 164.308(a)(5)(i), ''Security awareness and training.''

• Removed proposed § 142.308(a)(8), ''Security configuration management,'' and all implementation features, except ''Documentation'' (hardware and/or software installation, Inventory, Security testing, and Virus checking), since this requirement was determined to be redundant. ''Documentation'' has been made a discrete standard at § 164.316.

• Moved proposed § 142.308(a)(9), ''Security incident procedures,'' to § 164.308(a)(6)(i) and reworded for clarity. Combined ''Report procedures'' and ''Response procedures'' features into a single required implementation specification, named ''Response and Reporting'' at § 164.308(a)(6)(ii).

• Moved proposed § 142.308(a)(10), ''Security management process,'' to § 164.308(a)(1).

• Moved proposed § 142.308(a)(10)(i), ''Risk analysis,'' to § 164.308(a)(1)(ii)(A).

• Moved proposed § 142.308(a)(10)(ii), ''Risk management,'' to § 164.308(a)(1)(ii)(B).

• Moved proposed § 142.308(a)(10)(iii), ''Sanction policy,'' to § 164.308(a)(1)(ii)(C).

• Removed proposed § 142.308(a)(10)(iv), ''Security policy,'' since this requirement was determined to be redundant.

• Moved proposed § 142.308(a)(11), ''Termination,'' to § 164.308(a)(3)(ii)(C) as an addressable implementation specification under the ''Workforce security'' standard, and renamed as ''Termination procedures''. Removed ''Termination'' implementation features (changing locks, removal from access lists, removal of user accounts, turning in of keys, tokens, or cards) since these were determined to be too specific.

• Moved proposed § 142.308(a)(12), ''Training,'' to § 164.308(a)(5)(i) and renamed as ''Security awareness and training.'' Language modified to incorporate all training information under this one standard. Revised and made addressable all implementation specifications under this standard.

• Moved proposed § 142.308(b), ''Physical safeguards to guard data integrity, confidentiality and availability,'' to § 164.310 and renamed as ''Physical safeguards.'' Removed specific reference to locks and keys.

• Moved proposed § 142.308(b)(1), ''Assigned security responsibility requirement,'' to § 164.308(a)(2) since this has been determined to be an administrative procedure. Modified language to clarify that responsibility could be assigned to more than one individual.

• Moved proposed § 142.308(b)(2), ''Media controls,'' to § 164.310(d)(1) and renamed as ''Device and media controls.'' Removed the word ''formal.'' Added ''Media re-use'' as a required implementation specification at § 164.310(d)(2)(ii).

• Removed proposed § 142.308(b)(2)(i), ''Access control,'' implementation feature as it was determined to be redundant.

• Moved proposed § 142.308(b)(2)(ii), ''Accountability'' implementation feature to § 164.310(d)(2)(iii), and made it an addressable implementation specification.

• Combined proposed § 142.308(b)(2)(iii), ''Data backup,'' implementation feature with proposed § 142.308(b)(2)(iv), ''Data storage'' implementation feature, renamed as ''Data backup and storage'', moved to § 164.310(d)(2)(iv), and made it an addressable implementation specification.

• Moved proposed § 142.308(b)(2)(v), ''Data disposal,'' implementation feature to § 164.310(d)(2)(i) and made it a required implementation specification.

• Moved proposed § 142.308(b)(3),''Physical access controls,'' to § 164.310(a)(1) and renamed as ''Facility access controls.'' Removed word ''formal.''

• Moved proposed § 142.308(b)(3)(i), ''Disaster recovery,'' implementation feature to § 164.310(a)(2)(i). It is now part of the ''Contingency operations'' implementation specification.

• Moved proposed § 142.308(b)(3)(ii), ''Emergency mode operations,'' implementation feature to § 164.310(a)(2)(i). It is now part of the ''Contingency operations'' implementation specification.

• Removed proposed § 142.308(b)(3)(iii), ''Equipment control (into and out of site),'' as this information is now covered under § 164.310(d)(1), ''Device and media controls.''

• Moved proposed § 142.308(b)(3)(iv), ''A facility security plan,'' to § 164.310(a)(2)(ii).

• Moved proposed § 142.308(b)(3)(v), ''Procedure for verifying access authorizations,'' to § 164.310(a)(2)(iii) and renamed as ''Access control and validation procedures.'' Removed the word ''formal'' from text.

• Moved proposed § 142.308(b)(3)(vi), ''Maintenance records,'' to § 164.310(a)(2)(iv).

• Moved proposed § 142.308(b)(3)(vii), ''Need to know procedures for personnel access,'' to sect; 164.310(a)(2)(iii) and renamed as ''Access control and validation procedures.''

• Moved proposed § 142.308(b)(3)(viii), ''Procedures to sign in visitors and provide escort, if appropriate,'' to § 164.310(a)(2)(iii) and renamed as ''Access control and validation procedures.''

• Moved proposed § 142.308(b)(3)(ix), ''Testing and revision,'' to § 164.310(a)(2)(iii) and renamed as ''Access control and validation procedures.''

• Moved proposed § 142.308(b)(4), ''Policy and guidelines on workstation use,'' to § 164.310(b) and renamed as ''Workstation use.''

• Moved proposed § 142.308(b)(5), ''Secure work station location,'' to § 164.310(c) and renamed as ''Workstation security.''

• Removed proposed § 142.308(b)(6), ''Security awareness training,'' as a separate requirement. This requirement has been incorporated under § 164.308(a)(5)(i), ''Security awareness and training.''

• Combined and moved proposed § 142.308(c) and § 142.308(d), ''Technical security services to guard data integrity, confidentiality and availability'' and ''Technical security mechanisms,'' to § 164.312 and renamed as ''Technical safeguards.''

• Removed proposed § 142.308(c)(1) since it is no longer pertinent.

• Moved proposed § 142.308(c)(1)(i), ''Access control,'' to § 164.312(a)(1).

• Moved proposed § 142.308(c)(1)(i)(A), ''Procedure for emergency access,'' to § 164.312(a)(2)(ii), and renamed as ''Emergency access procedures.''

• Removed proposed § 142.308(c)(1)(i)(B).

• Removed proposed § 142.308(c)(1)(i)(B)(1), ''Context-based access,'' § 142.308(c)(1)(i)(B)(2), ''Role-based access,'' and § 142.308(c)(1)(i)(B)(3), ''User-based access,'' since these features were deemed too specific and were perceived as the only options permissible.

• Moved proposed § 142.308(c)(1)(i)(C), ''Optional use of encryption,'' to § 164.312(a)(2)(iv) and retitled ''Encryption and decryption.''

• Moved proposed § 142.308(c)(1)(ii), ''Audit controls,'' to § 164.312(b).

• Removed proposed § 142.308(c)(1)(iii), ''Authorization control,'' and all implementation features (Role-based access, User-based access) since this function has been incorporated into § 164.308(a)(4), ''Information access management.''

• Moved proposed § 142.308(c)(1)(iv), ''Data authentication,'' to § 164.312(c)(1), and retitled as ''Integrity.'' Reworded part of description and placed in § 164.312(c)(2), ''Mechanism to authenticate data,'' a new, addressable implementation specification. Removed reference to double keying.

• Moved proposed § 142.308(c)(1)(v), ''Entity authentication,'' to § 164.312(d) and retitled as ''Person or entity authentication.''

• Moved proposed § 142.308(c)(1)(v)(A), ''Automatic logoff,'' to § 164.312(a)(2)(iii).

• Moved proposed § 142.308(c)(1)(v)(B), ''Unique user identification,'' to § 164.312(a)(2)(i).

• Removed proposed § 142.308(c)(1)(v)(C) since text is no longer pertinent.

• Removed proposed § 142.308(c)(1)(v)(C)(2), ''Password,'' as too specific.

• Removed proposed § 142.308(c)(1)(v)(C)(3), ''PIN,'' as too specific.

• Removed proposed § 142.308(c)(1)(v)(C)(4), ''Telephone callback,'' as too specific.

• Removed proposed § 142.308(c)(1)(v)(C)(5), ''Token,'' as too specific.

• Removed proposed § 142.308(c)(2), as no longer relevant.

• Moved proposed § 142.308(d)(1), ''Communications or network controls,'' to § 164.312(e)(1) and renamed as ''Transmission security.''

• Removed proposed § 142.308(d)(1)(i), since it is no longer pertinent.

• Moved proposed § 142.308(d)(1)(i)(A), ''Integrity controls,'' to § 164.312(e)(2)(i) and reworded for clarity.

• Removed proposed § 142.308(d)(1)(i)(B), ''Message authentication,'' since this subject is now covered under § 164.312(e)(2)(i), ''Integrity controls.''

• Removed proposed § 142.308(d)(1)(ii) text since it is no longer pertinent.

• Removed proposed § 142.308(d)(1)(ii)(A), ''Access controls.''

• Moved proposed § 142.308(d)(1)(ii)(B), ''Encryption,'' to § 164.312(e)(2)(ii) and reworded to enhance flexibility and scalability.

• Removed proposed § 142.308(d)(2) text regarding: ''Network controls,'' and all implementation features (''Alarm,'' ''Audio trail,'' ''Entity authentication,'' ''Event reporting'').

• Removed proposed § 142.310, ''Electronic signature,'' and all subheadings. This section will be issued as a separate future regulation.

• Moved proposed § 142.310 ''Electronic signature Standard,'' to § 164.310. Where this section was proposed to contain the electronic signature standard, it now encompasses the ''Physical safeguards.''

• Moved proposed § 142.312, ''Effective date of the implementation of the security and electronic signature standards,'' to § 164.318 and retitled as ''Compliance dates for the initial implementation of the security standards.'' Reworded and retitled subsections.

• Added § 164.105, ''Organizational requirements,'' with two standards, ''Health care component and ''Affiliated covered entities'' with related implementation specifications.

• Added § 164.310(d)(2)(ii), ''Media re-use procedures,'' implementation specification.

• Added § 164.312, ''Technical safeguards,'' encompassing the combined technical services and technical mechanisms standards (proposed § 142.308(c) and (d)).

• Added § 164.314, ''Organizational requirements.''

• Added § 164.314(a)(1), ''Business associate contracts or other arrangements'' standard and related implementation specifications.

• Added § 164.314(b)(1), ''Requirements for group health plans'' standard and related implementation specifications.

• Added § 164.316, ''Policies and procedures and documentation requirements.''

• Added § 164.316(a), ''Policies and procedures'' standard.

• Added § 164.316(b)(1), ''Documentation'' standard and related implementation specifications.

• Added § 164.318, ''Compliance dates for the initial implementation of the security standards.''

• Renamed Addendum 1 as Appendix A.

• Removed Addendum 2. Definitions of terms used in this final rule are now incorporated into § 164.103 and § 164.304, or within the rule itself.

• Removed Addendum 3.

V. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), we are required to provide 30-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995 (PRA) requires that we solicit comment on the following issues:

• The need for the information collection and its usefulness in carrying out the proper functions of our agency.

• The accuracy of our estimate of the information collection burden.

• The quality, utility, and clarity of the information to be collected.

• Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

As discussed below, we are soliciting comment on the recordkeeping requirements, as referenced in § 164.306, § 164.308, § 164.310, § 164.314, and § 164.316 of this document.

Section 164.306 Security Standards: General Rules

Under paragraph (d), a covered entity must, if implementing the implementation specification is not reasonable and appropriate, document why it would not be reasonable and appropriate to implement the implementation specification.

We estimate that 75,000 entities will be affected by this requirement and that they will have to create documentation 3 times for this requirement. We estimate each instance of documentation will take .25 hours, for a one-time total burden of 56,250 hours.

Section 164.308 Administrative Safeguards

Under this section, a covered entity must document known security incidents and their outcomes.

We estimate that there will be 50 known incidents annually and that it will take 8 hours to document this requirement, for an annual burden of 400 hours.

This section further requires that each entity have a contingency plan, with specified components.

We estimate that there will be 60,000 entities affected by this requirement and that it will take each entity 8 hours to comply, for a total one-time burden of 480,000 hours.

This section also requires that the written contract or other arrangement with a business associate document the satisfactory assurances that the business associate will appropriately safeguard the information through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to document their arrangements via written contracts and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

Section 164.310 Physical Safeguards

This section requires that a covered entity implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).

We believe that 15,500 entities will have to repair or modify physical components, most of which will need to be done in the first year of implementation. In the following years, we estimate that 500 entities will need to make repairs or modifications. We estimate that it will take 10 minutes to document each repair or modification for a burden of 2,583 hours the first year and 83 hours annually subsequently.

This section requires that a covered entity create a retrievable, exact copy of electronic protected health information, where needed, before movement of equipment.

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to backup their data files, and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

Section 164.314 Organizational Requirements

This section requires that a covered entity report to the Secretary problems with a business associate's pattern of an activity or practice of the business associate that constitute a material breach or violation of the business associate's obligation under the contract or other arrangement if it is not feasible to terminate the contract or arrangement.

We believe that 10 entities will need to comply with this reporting requirement and that it will take them 60 minutes to comply with this requirement for an annual burden of 10 hours.

This section also requires that a covered entity may, if a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

We believe that this situation will affect 20 entities and that it will take 60 minutes to document attempts to obtain assurances and the reasons they cannot be obtained for an annual burden of 20 hours.

This section further requires that business associate contracts or other arrangements and group health plans must require the business entity and plan sponsor, respectively, to report to the covered entity any security incident of which it becomes aware.

We believe that the burden associated with this requirement is not subject to the PRA. It is good business practice for entities to document their agreements via written contracts, and as such is usual and customary among the entities subject to them. A burden associated with a requirement conducted in the normal course of business is exempt from the PRA as defined in 5 CFR 1320.3(b)(2).

Section 164.316 Policies and Procedures and Documentation Requirements

Paragraph (b)(1), *Standard: Documentation*, of this section requires a covered entity to—

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity, assessment, or designation is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, assessment, or designation.

We estimate that it will take the 4,000,000 entities covered by this final rule 16 hours to document their policies and procedures, for a total one-time burden of 64,000,000 hours.

The total annual burden of the information collection requirements contained in this final rule is 64,539,264 hours. These information collection requirements will be submitted to OMB for review under the PRA and will not become effective until approved by OMB.

If you comment on these information collection and recordkeeping requirements, please mail copies directly to the following:

Centers for Medicare and Medicaid Services, Office of Strategic Operations and Regulatory Affairs, Regulations Development and Issuances Group, Attn: Reports

Clearance Officer, 7500 Security Boulevard, Baltimore, MD 21244–1850, Attn: Julie Brown, CMS–0049–F; and

Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503, Attn: Brenda Aguilar, CMS Desk Officer.

IV. Regulatory Impact Analysis

A. Overall Impact

We have examined the impacts of this rule as required by Executive Order 12866 (September 1993, Regulatory Planning and Review), the Regulatory Flexibility Act (RFA) (September 16, 1980, Pub. L. 96–354), section 1102(b) of the Social Security Act, the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4), and Executive Order 13132.

Executive Order 12866 (as amended by Executive Order 13258, which merely reassigns responsibility of duties) directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any 1 year). Although we cannot determine the specific economic impact of the standards in this final rule (and individually each standard may not have a significant impact), the overall impact analysis makes clear that, collectively, all the standards will have a significant impact of over $100 million on the economy. Because this rule affects over 2 million entities, a requirement as low as $50 per entity would render this rule economically significant. This rule requires each of these entities to engage in, for example, at least some risk assessment activity; thus, this rule is almost certainly economically significant even though we do not have an estimate of the marginal impact of the additional security standards. However, the standards adopted in this rule are considerably more flexible than those anticipated in the overall impact analysis. Therefore, their implementation costs should be lower than those assumed in the impact analysis.

The RFA requires agencies to analyze options for regulatory relief of small businesses. For purposes of the RFA, small entities include small businesses, nonprofit organizations, and government agencies. Most hospitals and most other providers and suppliers are small entities, either by nonprofit status or by having revenues of $6 million to $29 million in any 1 year. While each standard may not have a significant impact on a substantial number of small entities, the combined effects of all the standards are likely to have a significant effect on a substantial number of small entities. Although we have certified this rule as having a significant impact, we have previously discussed the impact of small entities in the RFA published as part of the August 17, 2000 final regulation for the Standards for Electronic Transactions (65 FR 50312), on pages 50359 through 50360. That analysis included the impact of the set of HIPAA standards regulations (transactions and code sets, identifiers, and security). Although we discussed the impact on small entities in the previous analysis, we would like to discuss how this final rule has been structured to minimize the impact on small entities, compared to the proposed rule.

The proposed rule mandated 69 implementation features for all entities. A large number of commenters indicated that mandating such a large number would be burdensome for all entities. As a result, we have restructured this final rule to permit greater flexibility. While all standards must be met, we are now only requiring 13 implementation specifications. The remainder of the implementation specifications is ''addressable.'' For addressable specifications, an entity decides whether each specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision is based on a variety of factors, for example, the entity's risk analysis, what measures are already in place, the particular interest to small entities, and the cost of implementation.

Based on the decision, an entity can—(1) implement the specification if reasonable and appropriate; (2) implement an alternative security measure to accomplish the purposes of the standard; or (3) not implement anything if the specification is not reasonable and appropriate and the standard can still be met.

This approach will provide flexibility for all entities, and especially small entities that would be most concerned about the cost and complexity of the security standards. Small entities can look at the addressable implementation specifications and tailor their compliance based on their risks and capabilities of addressing those risks.

The required risk analysis is also a tool to allow flexibility for entities in meeting the requirements of this final rule. The risk analysis requirement is designed to allow entities to look at their own operations and determine the security risks involved. The degree of response is determined by the risks identified. We assume that smaller entities, who deal with smaller amounts of information would have smaller physical facilities, smaller work forces, and therefore, would assume less risk. The smaller amount of risk involved means that the response to that risk can be developed on a smaller scale than that for larger organizations.

Individuals and States are not included in the definition of a small entity. However, the security standards will affect small entities, such as providers and health plans, and vendors in much the same way as they affect any larger entities. Small providers who conduct electronic transactions and small health plans must meet the provisions of this regulation and implement the security standards. A more detailed analysis of the impact on small entities is part of the impact analysis published on August 17, 2000 (65 FR 50312), which provided the impact for all of the HIPAA standards, except privacy. As we discussed above, the scalability factor of the standards means that the requirements placed upon small providers and plans would be consistent with the complexity of their operations. Therefore, small providers and plans with appropriate security processes in place would need to do relatively little in order to comply with the standards. Moreover, small plans will have an additional year to come into compliance.

In addition, section 1102(b) of the Act requires us to prepare a regulatory impact analysis if a rule may have a significant impact on the operations of a substantial number of small rural hospitals. This analysis must conform to the provisions of section 604 of the RFA. For purposes of section 1102(b) of the Act, we define a small rural hospital as a hospital that is located outside of a Metropolitan Statistical Area and has fewer than 100 beds. While this rule may have a significant impact on small rural hospitals, the impact should be minimized by the scalability factors of the standards, as discussed above in the impact on all small entities. In addition, we have previously discussed the impact of small entities in the RIA published as part of the August 17, 2000 final regulation for the Standards for Electronic Transactions.

Section 202 of the Unfunded Mandates Reform Act (UMRA) of 1995

also requires that agencies assess anticipated costs and benefits before issuing any rule that may result in expenditure in any 1 year by State, local, or tribal governments, in the aggregate, or by the private sector, of $110 million. We estimate that implementation of all the standards will require the expenditure of more than $110 million by the private sector. Therefore, the rule establishes a Federal private sector mandate and is a significant regulatory action within the meaning of section 202 of UMRA (2 U.S.C. 1532). We have included the statements to address the anticipated effects of these rules under section 202.

These standards also apply to State and local governments in their roles as health plans or health care providers. Because these entities, in their roles as health plans or providers, must implement the requirements in these rules, the rules impose unfunded mandates on them. Further discussion of this issue can be found in the previously published impact analysis for all standards (65 FR 50360 through 50361).

The anticipated benefits and costs of the security standards, and other issues raised in section 202 of the UMRA, are addressed in the analysis below, and in the combined impact analysis. In addition, as required under section 205 of the UMRA (2 U.S.C. 1535), having considered a reasonable number of alternatives as outlined in the preamble to this rule, HHS has concluded that this final rule is the most cost-effective alternative for implementation of HHS's statutory objective of administrative simplification.

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications. The proposed rule was published before the enactment of Executive Order 13132 of August 4, 1999, Federalism (published in the **Federal Register** on August 10, 1999 (64 FR 43255)), which required meaningful and timely input by State and local officials in the development of rules that have Federalism implications). However, we received and considered comments on the proposed rule from State agencies and from entities who conduct transactions with State agencies. Several of the comments referred to the costs that will result from implementation of the HIPAA standards. As we stated in the impact analysis, we are unable to estimate the cost of implementing security features as implementation needs will vary dependent upon a risk assessment and upon what is already in place. However, the previously referenced impact analysis in the August 17, 2000 final rule (65 FR 50312) showed that Administrative Simplification costs will be offset by future savings.

In complying with the requirements of part C of title XI, the Secretary established interdepartmental implementation teams who consulted with appropriate State and Federal agencies and private organizations. These external groups consisted of the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Standards and Security, the Workgroup for Electronic Data Interchange (WEDI), the National Uniform Claim Committee (NUCC), the National Uniform Billing Committee (NUBC), and the American Dental Association (ADA). The teams also received comments on the proposed regulation from a variety of organizations, including State Medicaid agencies and other Federal agencies.

B. Anticipated Effects

The analysis in the August 2000, Transaction Rule included the expected costs and benefits of the administrative simplification regulations related to electronic systems for 10 years. Although only the electronic transaction standards were promulgated in the transaction rule, HHS expected affected parties to make systems compliance investments collectively because the regulations are so integrated. Moreover, the data available to us were also based on the collective requirements of this regulation. It is not feasible to identify the incremental technological and computer costs for each regulation. Although HHS is issuing rules under HIPAA sequentially, affected entities and vendors are bundling services, that is, they have been anticipating the various needs and are designing relatively comprehensive systems as they develop hardware and software. For example, a vendor developing a system for electronic billing would also anticipate and include security features, even in the absence of any regulation. Moreover, a draft of the security rule was first published in 1998. Even though the final is different (and less burdensome), vendors had a reasonable indication of the direction policy would go. Thus, in preparing the electronic transaction rule, we recognized and included costs that might theoretically be associated with security or other HIPPA rules. Hence, some of the ''costs'' of security have already been accounted for in the Standards for Electronic Transactions cost estimate (45 CFR parts 160 and 162), which was published in the **Federal Register** on August 17, 2000 (65 FR 50312).

This analysis showed that the combined impact of the Administrative Simplification standards is expected to save the industry $29.9 billion over 10 years. We are including in each subsequent rule an impact analysis that is specific to the standard or standards in that rule, but the impact analysis will assess only the incremental cost of implementing a given standard over another. Thus, the following discussion contains the impact analysis for the marginal costs of the security standards in this final rule.

The following describes the specific impacts that relate to the security standards. The security of electronic protected health information is, and has been for some time, a basic business requirement that health care entities ignore at their peril. Instances of ''hacking'' and other security violations may be widely publicized, and can seriously damage an institution's community standing. Appropriate security protections are crucial for encouraging the growth and use of electronic data interchange. The synergistic effect of the employment of the security standards will enhance all aspects of HIPAA's Administrative Simplification requirements. In addition, it is important to recognize that security is not a one-time project, but rather an on-going, dynamic process.

C. Changes From the 1998 Impact Analysis

The overall impact analysis for Administrative Simplification was first published on May 7, 1998 (63 FR 25320) in the proposed rule for the National Provider Identifier standard (45 CFR part 142), the first of the proposed Administrative Simplification rules. That impact analysis was based on the industry situation at that time, used statistics which were current at that time, and assumed that all of the HIPAA standards would be implemented at roughly the same time, which would permit software changes to be made less expensively. While the original impact analysis represented our best information at that time, we realize that the state of the industry, and of security technology, has changed since 1998. We discuss several of those changes and how they affect the impact of this regulation.

1. Changes in Technology

The state of technology for health care security has changed since 1998. New

technologies to protect information have been developed over the past several years. As a result, HHS has consulted with the Gartner Group, a leading technology assessment organization, regarding what impact these changes in the industry might have on the expected impact of this regulation. The Gartner analysis indicated that the cost of meeting the requirements of a reasonable interpretation of the security rule in 2002 is probably less than 10 percent higher in 2002 than it was in 1998. This increase is mainly driven by more active threats and increased personnel costs offsetting decreases in technology costs over the past 4 years. However, spending by companies who have anticipated the security rule or who have independently made business decisions to implement security policies and procedures as good business practice(s) has already occurred, and probably will cancel out the increased costs of implementation. Therefore, Gartner expects the cost of complying with the HIPAA security standards to be about the same now as it was in 1998.

2. Synchronizing Standards

The timelines for the implementation of the initial HIPAA standards (transactions, identifiers, and security) are no longer closely synchronized. However, we do not believe that this lack of synchronization will have a significant impact on the cost of implementing security. The analysis provided by the Gartner group indicated that implementing security standards is being viewed by entities as a separate task from implementing the transaction standards, and that this is not having a significant impact on costs. As with other HIPAA standards, most current entities will have a 2-year implementation period before compliance with the standards is required. Covered entities will develop their own implementation schedules, and may phase in various security measures over that time period.

3. Relationship to Privacy Standards

The publication of the final Privacy Rules (45 CFR parts 160 and 164) on December 28, 2000 in the **Federal Register** (65 FR 82462) and on August 14, 2002 (67 FR 53182) has affected the impact of this regulation significantly. Covered entities must implement the privacy standards by April 14, 2003 (April 14, 2004 for small health plans). The implementation of privacy standards reduces the cost of implementing the security standards in two significant areas.

First, we have made substantial efforts to ensure that the many requirements in the security standards parallel those for privacy, and can easily be satisfied using the solutions for privacy. Administrative requirements like the need for written policies, responsible officers, and business associate agreements that are already required by the Privacy Rule can also serve to meet the security standards without significant additional cost. The analysis of data flows and data uses that covered entities are doing so as to comply with the Privacy Rule should also serve as the starting point for parallel analysis required by this final rule.

Second, it is likely that covered entities will meet a number of the requirements in the security standards through the implementation of the privacy requirements. For example, in order to comply with the Privacy Rule requirements to make reasonable efforts to limit the access of members of the work force to specified categories of protected health information, covered entities may implement some of the administrative, physical, and technical safeguards that the entity's risk analysis and assessment would require under the Security Rule. E-mail authentication procedures put into place for privacy protection may also meet the security standards, thereby eliminating the need for additional investments to meet these standards. As a result, covered entities that have moved forward in implementing the privacy standards are also implementing security measures at the same time. Since the proposed security standards proposed rule represents the most authoritative guidance now available on the nature of these standards, some entities have been using them to develop their security measures. Those entities should face minimal incremental costs in implementing the final version of these standards.

We are unable to quantify these overlaps, but we believe they may reduce the cost of implementing these security standards. The analysis provided to the HHS by the Gartner Group also stated that compliance with the Privacy Rule will have a moderate effect on the cost of compliance with the Security Rule, reducing it slightly.

4. Sensitivity to Security Concerns as a Result of September 11, 2001

In our discussions with the Gartner Group, they indicated that they saw little evidence of increased security awareness in health care organizations as a result of the events of September 11, 2001. However, a survey conducted by Phoenix Health Systems in the winter of 2002 showed that 65 percent of the respondents to the survey (hospitals, payers, vendors, and clearinghouses) have moderately to greatly increased their attention on overall security. If these organizations have already made investments in security that meet some of the requirements of this rule, it will reduce their added costs of compliance. However, HHS can make no clear statement of the impact of this attention.

D. Guiding Principles for Standard Selection

The implementation teams charged with designating standards under the statute have defined, with significant input from the health care industry, a set of common criteria for evaluating potential standards. These criteria are based on direct specifications in the HIPAA, the purpose of the law, and principles that support the regulatory philosophy set forth in the E.O. 12866 of September 30, 1993, and the Paperwork Reduction Act of 1995. In order to be designated as such, a standard should do the following:

- Improve the efficiency and effectiveness of the health care system by leading to cost reductions for or improvements in benefits from electronic health care transactions. This principle supports the regulatory goals of cost-effectiveness and avoidance of burden.
- Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses. This principle supports the regulatory goal of cost-effectiveness.
- Be consistent and uniform with the other HIPAA standards (that is, their data element definitions and codes, and their privacy and security requirements) and, secondarily, with other private and public sector health data standards. This principle supports the regulatory goals of consistency and avoidance of incompatibility, and it establishes a performance objective for the standard.
- Have low additional development and implementation costs relative to the benefits of using the standard. This principle supports the regulatory goals of cost-effectiveness and avoidance of burden.
- Be supported by an ANSI-accredited standards developing organization or other private or public organization that would ensure continuity and efficient updating of the standard over time. This principle supports the regulatory goal of predictability.
- Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster. This

principle establishes a performance objective for the standard.

- Be technologically independent of the computer platforms and transmission protocols used in health transactions, except when they are explicitly part of the standard. This principle establishes a performance objective for the standard and supports the regulatory goal of flexibility.
- Be precise and unambiguous but as simple as possible. This principle supports the regulatory goals of predictability and simplicity.
- Keep data collection and paperwork burdens on users as low as is feasible. This principle supports the regulatory goals of cost-effectiveness and avoidance of duplication and burden.
- Incorporate flexibility to adapt more easily to changes in the health care infrastructure (for example, new services, organizations, and provider types) and information technology. This principle supports the regulatory goals of flexibility and encouragement of innovation.

We assessed a wide variety of security standards and guidelines against the principles listed above, with the overall goal of achieving the maximum benefit for the least cost. As we stated in the proposed rule, we found that no single standard for security exists that encompasses all the requirements that were listed in the law. However, we believe that the standards we are adopting in this final rule collectively accomplish these goals.

E. Affected Entities

1. Health Care Providers

Covered health care providers may incur implementation costs for establishing or updating their security systems. The majority of costs to implement the security standard (purchase and installation of appropriate computer hardware and software, and physical safeguards) would generally be incurred in the initial implementation period for the specific requirements of the security standard. Health care providers that do not conduct electronic transactions for which standards have been adopted are not affected by these regulations.

2. Health Plans

All health plans, as the term is defined in regulation at 45 CFR 160.103, must comply with these security standards. In addition, health plans that engage in electronic health care transactions may have to modify their systems to meet the security standards. Health plans that maintain electronic health information may also have to modify their systems to meet the security standards. This conversion would have a one-time cost impact on Federal, State, and private plans alike.

We recognize that this conversion process has the potential to cause business disruption of some health plans. However, health plans would be able to schedule their implementation of the security standards and other standards in a way that best fits their needs, as long as they meet the deadlines specified in the HIPAA law and regulations. Moreover, small plans (many of which are employer-sponsored) will have an additional year in which to achieve compliance. Small health plans are defined at 45 CFR 160.103 as health plans with annual receipts of $5 million or less.

3. Clearinghouses

All health care clearinghouses must meet the requirements of this regulation. Health care clearinghouses would face effects similar to those experienced by health care providers and health plans. However, because clearinghouses represent one way in which providers and plans can achieve compliance, the clearinghouses' costs of complying with these standards would probably be passed along to those entities, to be shared over the entire customer base.

4. System Vendors

Systems vendors that provide computer software applications to health care providers and other billers of health care services would likely be affected. These vendors would have to develop software solutions that would allow health plans, providers, and other users of electronic transactions to protect these transactions and the information in their databases from unauthorized access to their systems. Their costs would also probably be passed along to their customer bases.

F. Factors in Establishing the Security Standard

1. General Effect

In assessing the impact of these standards, it is first necessary to focus on the general nature of the standards, their scalability, and the fact that they are not dependent upon specific technologies. These factors will make it possible for covered entities to implement them with the least possible impact on resources. Because there is no national security standard in widespread use throughout the industry, adopting any of the candidate standards would require most health care providers, health plans, and health care clearinghouses to at least conduct an assessment of how their current security measures conform to the new standards. However, we assume that most, if not all, covered entities already have at least some rudimentary security measures in place. Covered entities that identify gaps in their current measures would need to establish or revise their security precautions.

It is also important to note that the standards specify what goals are to be achieved, but give the covered entity some flexibility to determine how to meet those goals. This is different from the transaction standards, where all covered entities must use the exact same implementation guide. With respect to security, covered entities will be able to blend security processes now in place with new processes. This should significantly reduce compliance costs.

Based on our analysis and comments received, the security standards adopted in this rule do not impose a greater burden on the industry than the options we did not select, and they present significant advantages in terms of universality and flexibility.

We understand that some large health plans, health care providers, and health care clearinghouses that currently exchange health information among trading partners may already have security systems and procedures in place to protect the information from unauthorized access. These entities may not incur significant costs to meet the security standards. Large entities that have sophisticated security systems in place may only need minor revisions or updates to their systems to meet the security standards, or indeed, may not need to make any changes in their systems.

While small providers are not likely to have implemented sophisticated security measures, they are also not as likely to need them as larger covered entities. The scalability principle allows providers to adopt measures that are appropriate to their own circumstances.

2. Complexity of Conversion

The complexity of the conversion to the security standards could be significantly affected by the volume of transactions that covered entities transmit and process electronically and the desire to transmit directly or to use the services of a Value Added Network (VAN) or a clearinghouse. If a VAN or clearinghouse is used, some of the conversion activities would be carried out by that organization, rather than by the covered entity. This would simplify conversion for the covered entity, but makes the covered entity dependent on the success of its business associate. The architecture, and specific technology

limitations of existing systems could also affect the complexity of the conversion (for example, certain practice management software that does not contain password protection will require a greater conversion effort than software that has a password protection option already built into it).

3. Cost of Conversion

Virtually all providers, health plans, and clearinghouses that transmit or store data electronically have already implemented some security measures and will need to assess existing security, identify areas of risk, and implement additional measures in order to come into compliance with the standards adopted in this rule. We cannot estimate the per-entity cost of implementation because there is no information available regarding the extent to which providers', plans', and clearinghouses' current security practices are deficient. Moreover, some security solutions are almost cost-free to implement (for example, reminding employees not to post passwords on their monitors), while others are not.

Affected entities will have many choices regarding how they will implement security. Some may choose to assess security using in-house staff, while others will use consultants. Practice management software vendors may also provide security consultation services to their customers. Entities may also choose to implement security measures that require hardware and/or software purchases at the time they do routine equipment upgrades.

The security standards we adopt in this rule were developed with considerable input from the health care industry, including providers, health plans, clearinghouses, vendors, and standards organizations. Industry members strongly advocated the flexible approach we adopt in this rule, which permits each affected entity to develop cost-effective security measures appropriate to their particular needs. We believe that this approach will yield the lowest implementation cost to industry while ensuring that electronic protected health information is safeguarded.

All of the nation's health plans (over 2 million) and providers (over 600,000) will need to conduct some level of gap analysis to assess current procedures against the standards. However, we cannot estimate the number of covered entities that would have to implement additional security systems and procedures to meet the adopted standards. Also, we are not able to estimate the number of providers that do not conduct electronic transactions today but may choose to do so at some future time (these would be entities that send and receive paper transactions and maintain paper records and thus would not be affected). We believe that the security standards represent the minimum necessary for adequate protection of health information in an electronic format and as such should be implemented by all covered entities. As discussed earlier in this preamble, the security requirements are both scalable and technically flexible; and while the law requires each health plan that is not a small plan to comply with the security and electronic signature requirements no later than 24 months after the effective date of the final rule, small plans will be allowed an additional 12 months to comply.

Since we are unable to estimate the number of entities that may need to make changes to meet the security standards, we are also unable to estimate the cost for those entities. However, we believe that the cost of establishing security systems and procedures is a portion of the costs associated with converting to the administrative simplification standards that are required under HIPAA, which are estimated in the previously referenced impact analysis.

This discussion on conversion costs relates only to health plans, health care providers, and health care clearinghouses that are required to implement the security standards. The cost of implementing security systems and procedures for entities that do not transmit, receive, or maintain health information electronically is not a cost imposed by the rule, and thus, is not included in our estimates.

G. Alternatives Considered

In developing this final rule, the Department considered some alternatives. One alternative was to not issue a final rule. However, this would not meet the Department's obligations under the HIPAA statute. It would also leave the health industry without a set of standards for protecting the security of health information. The vast majority of commenters supported our efforts in developing a set of standards. Thus, we concluded that not publishing a final rule was not in the best interests of the industry and not in the best interests of persons whose medical information will be protected by these measures.

A second alternative was to publish the final rule basically unchanged from the proposed rule. Although most commenters supported the approach of the proposed rule, there were significant objections to the number of required specifications, concerns about the scope of certain requirements, duplication and ambiguity of some requirements, and the overall complexity of the approach. Based on those comments, it was clear that revisions had to be made. In addition, the proposed rule was developed before the Privacy Rule requirements were developed. Thus, it did not allow for any alignment of requirements between the Privacy and Security standards.

As a result, the Department determined that an approach that modified the proposed rule and aligned the requirements with the Privacy standards was the preferred alternative.

V. Federalism

Executive Order 13132 of August 4, 1999, Federalism, published in the **Federal Register** on August 10, 1999 (64 FR 43255), requires us to ensure meaningful and timely input by State and local officials in the development of rules that have Federalism implications. Although the proposed rule for security standards was published before the enactment of this Executive Order, the Department consulted with State and local officials as part of an outreach program in the process of developing the proposed regulation. The Department received comments on the proposed rule from State agencies and from entities that conduct transactions with State agencies. Many of these comments were concerned with the burden that the proposed security standards would place on their organizations. In response to those comments, we have modified the security standards to make them more flexible and less burdensome.

In complying with the requirements of part C of Title XI, the Secretary established an interdepartmental team who consulted with appropriate State and Federal agencies and private organizations. These external groups included the NCVHS Workgroup on Standards and Security, the Workgroup for Electronic Data Interchange, the National Uniform Claim Committee, and the National Uniform Billing Committee. Most of these groups have State officials as members. We also received comments on the proposed regulation from these organizations.

In accordance with the provisions of Executive Order 12866, this rule has been reviewed by the Office of Management and Budget.

List of Subjects

45 CFR Part 160

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health

records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

45 CFR Part 162

Administrative practice and procedure, Health facilities, Health insurance, Hospitals, Medicaid, Medicare, report and recordkeeping requirement.

45 CFR Part 164

Administrative practice and procedure, Health facilities, Health insurance, Hospitals, Medicaid, Medicare, Electronic Information System, Security, Report and recordkeeping requirement.

For the reasons set forth in the preamble, the Department of Health and Human Services amends title 45, subtitle A, subchapter C, parts 160, 162, and 164 as set forth below:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 160 continues to read as follows:

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d–1329d–8) as added by sec. 262 of Pub. L. 104–191, 110 Stat. 2021–2031 and sec. 264 of Pub. L. 104–191 (42 U.S.C. 1320d–2(note)).

2. In § 160.103, the definitions of ''disclosure'', ''electronic media'', ''electronic protected health information,'' ''individual,'' ''organized health care arrangement'', ''protected health information,'' and ''use'' are added in alphabetical order to read as follows:

§ 160.103 Definitions.

* * * * *

Disclosure means the release, transfer, provision of, access to, or

divulging in any other manner of information outside the entity holding the information.

* * * * *

Electronic media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of *protected health information* as specified in this section.

* * * * *

Individual means the person who is the subject of protected health information.

* * * * *

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) *Protected health information* excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

* * * * *

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

* * * * *

PART 162—ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 162 is revised to read as follows:

Authority: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d–1320d–8), as added by sec. 262 of Pub. L. 104–191, 110 Stat. 2021–2031, and sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)).

§ 162.103 [Amended]

2. In § 162.103, the definition of ''electronic media'' is removed.

PART 164—SECURITY AND PRIVACY

1. The authority citation for part 164 is revised to read as follows:

Authority: Secs. 1171 through 1179 of the Social Security Act (42 U.S.C. 1320d–1320d–8), as added by sec. 262 of Pub. L. 104–191, 110 Stat. 2021–2031, and 42 U.S.C. 1320d–2 and 1320d–4, sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)).

2. A new § 164.103 is added to read as follows:

§ 164.103 Definitions.

As used in this part, the following terms have the following meanings:

Common control exists if an entity has the power, directly or indirectly,

significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(C).

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(C).

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

3. Section 164.104 is revised to read as follows:

§ 164.104 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, or other than as a business associate of a covered entity, the clearinghouse must comply with § 164.105 relating to organizational requirements for covered entities, including the designation of health care components of a covered entity.

4. A new § 164.105 is added to read as follows:

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of subparts C and E of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*

(i) *Application of other provisions.* In applying a provision of subparts C and E of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

(A) A reference in such provision to a ''covered entity'' refers to a health care component of the covered entity;

(B) A reference in such provision to a ''health plan,'' ''covered health care provider,'' or ''health care clearinghouse,'' refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to ''protected health information'' refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to ''electronic protected health information'' refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this section and subparts C and E of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) A component that is described by paragraph (a)(2)(iii)(C)(*2*) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by subpart E of this part;

(D) A component that is described by paragraph (a)(2)(iii)(C)(*2*) of this section that creates, receives, maintains, or transmits electronic protected health information on behalf of the health care component is in compliance with subpart C of this part; and

(E) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with subpart E of this part.

(B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this section and subparts C and E of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

(*1*) Covered functions; or

(*2*) Activities that would make such component a business associate of a

component that performs covered functions if the two components were separate legal entities.

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of subparts C and E of this part.

(1) *Implementation specifications:*

(i) *Requirements for designation of an affiliated covered entity.*

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of subparts C and E of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that:

(A) The affiliated covered entity's creation, receipt, maintenance, or transmission of electronic protected health information complies with the applicable requirements of subpart C of this part;

(B) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of subpart E of this part; and

(C) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

(c)(1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation as required by paragraph (c)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

5. A new subpart C is added to part 164 to read as follows:

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

Sec.

164.302 Applicability.
164.304 Definitions.
164.306 Security standards: General rules.
164.308 Administrative safeguards.
164.310 Physical safeguards.
164.312 Technical safeguards.
164.314 Organizational requirements.
164.316 Policies and procedures and documentation requirements.
164.318 Compliance dates for the initial implementation of the security standards.

Appendix A to Subpart C of Part 164—Security Standards: Matrix

Authority: 42 U.S.C. 1320d–2 and 1320d–4.

§ 164.302 Applicability.

A covered entity must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information.

§ 164.304 Definitions.

As used in this subpart, the following terms have the following meanings:

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to ''access'' as used in this subpart, not as used in subpart E of this part.)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) *Flexibility of approach.*

(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) *Standards.* A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications.* In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word ''Required'' appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word ''Addressable'' appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.

(1) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

(ii) As applicable to the entity—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) *Maintenance.* Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.

§ 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with § 164.306:

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) *Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3)(i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) *Standard: Information access management.* Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications*:

(A) *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5)(i) *Standard: Security awareness and training.* Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications.* Implement:

(A) *Security reminders* (Addressable). Periodic security updates.

(B) *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6)(i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.

(ii) *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

(7)(i) *Standard: Contingency plan.* Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

(b)(1) *Standard: Business associate contracts and other arrangements.* A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

(2) This standard does not apply with respect to—

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) *Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

§ 164.310 Physical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) *Standard: Facility access controls.* Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) *Implementation specifications:*

(i) *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) *Facility security plan* (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use.* Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) *Standard: Workstation security.* Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) *Standard: Device and media controls.* Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) *Implementation specifications:*

(i) *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§ 164.312 Technical safeguards.

A covered entity must, in accordance with § 164.306:

(a)(1) *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) *Implementation specifications:*

(i) *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) *Standard: Integrity.* Implement policies and procedures to protect

electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls* (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements.*

(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) *Implementation specifications* (Required).

(i) *Business associate contracts.* The contract between a covered entity and a business associate must provide that the business associate will—

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(ii) *Other arrangements.*

(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if—

(*1*) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or

(*2*) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.

(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

(C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(b)(1) *Standard: Requirements for group health plans.* Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation specifications* (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

§ 164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with § 164.306:

(a) *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) *Standard: Documentation.*

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications:*

(i) *Time limit* (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability* (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates* (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

§ 164.318 Compliance dates for the initial implementation of the security standards.

(a) *Health plan.*

(1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

Appendix A to Subpart C of Part 164—Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

§164.500 [Amended]

6. § In 164.500(b)(1)(iv), remove the words ''including the designation of health care components of a covered entity''.

§ 165.501 [Amended]

7. In §164.501, the definitions of the following terms are removed: *Covered functions, Disclosure, Individual, Organized health care arrangement, Plan sponsor Protected health information, Required by law,* and *Use.*

§ 164.504 [Amended]

8. In §164.504, the following changes are made:

a. The definitions of the following terms are removed: *Common control, Common ownership, Health care component,* and *Hybrid entity.*

b. Paragraphs (b) through (d) are removed and reserved.

Authority: Sections 1173 and 1175 of the Social Security Act (42 U.S.C. 1329d–2 and 1320–4).

Dated: January 13, 2003.

Tommy G. Thompson,

Secretary.

[FR Doc. 03–3877 Filed 2–13–03; 8:45 am]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 162

[CMS–0003–F and CMS–0005–F]

RINs 0938–AK64 and 0938–AK76

Health Insurance Reform: Modifications to Electronic Data Transaction Standards and Code Sets

AGENCY: Office of the Secretary, HHS.

ACTION: Final rule.

SUMMARY: In this final rule, we respond to public comments received and finalize provisions applicable to electronic data transaction standards from two related proposed rules published in the May 31, 2002, **Federal Register.** We are also adopting proposed modifications to implementation specifications for health care entities and others. In addition, we are adopting modifications to implementation specifications for several electronic transaction standards that were omitted from the May 31, 2002, proposed rules.

EFFECTIVE DATES: These regulations are effective on March 24, 2003. The incorporation by reference of certain publications listed in this final rule is approved by the Director of the Federal Register as of March 24, 2003.

FOR FURTHER INFORMATION CONTACT: Gladys Wheeler, (410) 786–0273.

SUPPLEMENTARY INFORMATION: *Availability of Copies:* To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512–1800 (toll-free at 1–888–293–6498) or by faxing to (202) 512–2250. The cost for each copy is $10. As an alternative, you can view and photocopy the **Federal Register** document at most libraries designated as Federal Depository Libraries and at many other public and academic libraries throughout the country that receive the Federal Register. This **Federal Register** document is also available from the **Federal Register** online database through *GPO Access,* a service of the U.S. Government Printing Office. The Web site address is: *http://www.access.gpo.gov/nara/index.html.*

I. Background

A. Electronic Data Interchange

Electronic data interchange (EDI) refers to the electronic transfer of information in a standard format between trading partners. When compared with paper submissions, EDI can substantially lessen the time and costs associated with receiving, processing, and storing documents. The use of EDI can also eliminate inefficiencies and streamline processing tasks, which can in turn result in less administrative burden, lower operating costs, and improved overall data quality.

The health care industry recognizes the benefits of EDI, and many entities in the industry have developed proprietary EDI formats. However, with the increasing use of health care EDI standards, the lack of common, industry-wide standards has emerged as a major obstacle to realizing potential efficiency and savings.

B. Statutory and Regulatory Background

1. Statutory Background

The Congress included provisions to address the need for developing a consistent framework for electronic transactions and other administrative simplification issues in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191, which became law on August 21, 1996. Through subtitle F of title II of that statute, the Congress added to title XI of the Social Security Act (the Act) a new part C, titled ''Administrative Simplification.'' The purpose of this part is to improve the Medicare and Medicaid programs in particular and the efficiency and effectiveness of the health care system in general, by encouraging the development of standards and requirements to enable the electronic exchange of certain health information.

Part C of title XI consists of sections 1171 through 1179 of the Act. Section 1172 of the Act and the implementing regulations make any standard adopted under part C applicable to: (1) Health plans; (2) health care clearinghouses; and (3) health care providers who transmit any health information in electronic form in connection with a transaction covered by 45 CFR part 162.

In general, section 1172 of the Act requires any standard adopted by the Secretary of Health and Human Services (the Secretary) under this part to be a standard that has been developed, adopted, or modified by a standard setting organization (SSO). The Secretary may adopt a different standard if the standard will substantially reduce administrative costs to providers and health plans compared to the alternatives, and the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5, U.S.C.

Section 1172 of the Act also sets forth consultation requirements that must be met before the Secretary may adopt standards. In the case of a standard that is developed, adopted, or modified by an SSO, the SSO must consult with the following Data Content Committees (DCCs) in the course of the development, adoption, or modification of the standard: The National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC), the Workgroup for Electronic Data Interchange (WEDI), and the American Dental Association (ADA). In the case of any other standard, the Secretary is required to consult with each of the above-named groups before adopting the standard and must also comply with the provisions of section 1172(f) of the Act regarding consultation with the National Committee on Vital and Health Statistics (NCVHS).

Section 1173 of the Act requires the Secretary to adopt standards for transactions, and data elements for such transactions, to enable the electronic exchange of health information. Section

Attachment J.17

Request For Disenrollment of DC Medicaid Recipient Requiring Long-Term Care

Recipient' s Name: _____

Recipient' s Date of Birth: _____

Recipient' s Medicaid Number: _____

Recipient' s Social Security Number: _____

Current Health Plan: _____

Recipient' s diagnosis: _____

Name, address, and phone number of treating facility:

_____

_____

_____

Date of admission: _____

Anticipated length of stay: _____

Reason for disenrollment request: _____

Proposed effective date of disenrollment: _____

Status of SSI filing on behalf of member: _____

Filed by: _____ _____

(Print name) (Date of request)

_____ _____ _____

(Organization) (Phone number) (Fax number)

Form should be faxed to Sylvia Cobbs, Office of Managed Care/Medicaid

(202) 478-1379

Attachment J.18

List of Electronic Resources for Applicable Law, Section C.1.2.1

Federal statutory and regulatory citations may be located at:

Title XIX of Social Security Act
http://www.ssa.gov/OP_Home/ssact/title19/1900.htm

Balanced Budget Act P.L. 105-33 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ33.105.pdf

42 U.S.C. §1320a-3
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1320a-3

42 U.S.C. §1320a-7
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1320a-7

42 U.S.C. §1320a-7a
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1320a-7a

42 U.S.C. §1320a-7b
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1320a-7b

42 U.S.C. §1320d-2
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1320d-2

42 U.S.C. §1396a
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1396a

42 U.S.C. §1395dd
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1395dd

42 U.S.C. §1396d
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1396d

42 U.S.C. §1396r-8
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1396r-8

Attachment J.18

42 U.S.C. §1396ru-2
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1396u-2

42 U.S.C. §1396n (b)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1396n

42 U.S.C. §1315
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC1315

29U.S.C. §794
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+29USC794

42 U.S.C. §12101
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC12101

42 C.F.R Part 2
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr2_05.html

State Organization and General Administration
42 C.F.R part 422
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr422_05.html

42 C.F.R. Part 431
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr431_05.html

42 C.F.R. Part 434, Subpart F
http://a257.g.akamaitech.net/7/257/2422/09nov20051500/edocket.access.gpo.gov/cfr_2005/octqtr/pdf/42cfr434.70.pdf
and 42 CFR Part 434 et seq.
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr434_05.html

42 C.F.R Part 435
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr435_05.html

42 C.F.R. Part 438
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr438_05.html

42 C.F.R. Part 440
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr440_05.html

and 42 C.F.R. Part 441
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr441_05.html

42 C.F.R. Part 447
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr447_05.html

42 C.F.R. Part 489
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr489_05.html

42 C.F.R. Part 455
http://www.access.gpo.gov/nara/cfr/waisidx_05/42cfr455_05.html

Uniform administrative requirements for awards and subawards to institutions of higher education, hospitals, other nonprofit organizations, and commercial organizations; and certain grants and agreements with states, local governments and Indian tribal governments
45 C.F.R. Part 74 including appendix A
http://www.access.gpo.gov/nara/cfr/waisidx_05/45cfr74_05.html

All D.C. Code Citations may be found at the D.C. City Council website (http://www.dccouncil.washington.dc.us/) and, more specifically, at: http://government.westlaw.com/linkedslice/default.asp?rs=gvt1.0&vr=2.0&sp=dcc-1000.

Specific citations may be located as described below.

DC Code § 1-307.02
http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES1%2D307%2E02&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=dcc-1000&trailtype=26

DCMR Title 29 (not available online)

DC Code §31-3132
http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES31%2D3132&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=dcc-1000&trailtype=26

DC Code § 7-131
http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES7%2D131&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=dcc-1000&trailtype=26

DC Code § 7-132

http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES7%2D132&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=dcc-1000&trailtype=26

DCMR Title 22 (not available online)

DC Code § 7-871.03
http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES7%2D871%2E03&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=dcc-1000&trailtype=26

Annual Audited Financial Reports, Definitions
DC Code §31-301
http://weblinks.westlaw.com/Find/Default.wl?RP=%2FFind%2Fdefault%2Ewl&CanDisNum=1&CFID=1&Docname=DCCODES31%2D301&Findtype=W&n=1&NumSDUs=4&RLT=CLID%5FFQRLT5224102011&Service=Find&RS=WEBL6.11&VR=2.0&SPa=dcc-1000&DISNav=PREV&DISRelPos=1

Filing Requirements
DC Code §31-1901
http://weblinks.westlaw.com/Find/default.wl?CFID=0&DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES31%2D1901&FindType=W&fn=%5Ftop&n=1&rs=WEBL6%2E11&spa=dcc%2D1000&trailtype=26&vr=2%2E0&Action=DODIS&CanDisNum=1

Law on Examinations, Definitions
DC Code §31-1401
http://weblinks.westlaw.com/Find/default.wl?CFID=0&DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES31%2D1401&FindType=W&fn=%5Ftop&n=1&rs=WEBL6%2E11&spa=dcc%2D1000&trailtype=26&vr=2%2E0&Action=DODIS&CanDisNum=1

Holding Company System, Definitions
DC Code §31-701
http://weblinks.westlaw.com/Find/default.wl?CFID=0&DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES31%2D701&FindType=W&fn=%5Ftop&n=1&rs=WEBL6%2E11&spa=dcc%2D1000&trailtype=26&vr=2%2E0&Action=DODIS&CanDisNum=1

Standards for Determining Insurance Companies in Hazardous Financial Condition
DC Code §31-2101
http://weblinks.westlaw.com/Find/default.wl?CFID=0&DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES31%2D2101&FindType=W&fn=%5Ftop&n=1&rs=WEBL6%2E11&spa=dcc%2D1000&trailtype=26&vr=2%2E0&Action=DODIS&CanDisNum=1

Health Care Safety Net Administration Establishment
DC Code §7-1401
http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES7%2D1401&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=DCC-1000&trailtype=26

Authorization to Contract for Comprehensive Health Care Services
DC Code §7-1405
http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES7%2D1405&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=DCC-1000&trailtype=26

Medical Assistance Program
DC Code §1-307.02(d)(3) and (d)(5)
http://weblinks.westlaw.com/Find/Default.wl?DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES1%2D307%2E02&FindType=W&AP=&fn=_top&rs=WEBL6.11&vr=2.0&spa=DCC-1000&trailtype=26

DC Code §7-1201.01 – §7.1208.07
http://weblinks.westlaw.com/Find/default.wl?CFID=0&DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES7%2D1201%2E01&FindType=W&fn=%5Ftop&n=1&rs=WEBL6%2E11&spa=dcc%2D1000&trailtype=26&vr=2%2E0&Action=DODIS&CanDisNum=1

DC Code §3-1200
http://weblinks.westlaw.com/Find/default.wl?CFID=0&DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODEDIT3SUBTIC12R&FindType=W&fn=%5Ftop&n=1&rs=WEBL6%2E11&spa=dcc%2D1000&trailtype=26&vr=2%2E0&Action=DODIS&CanDisNum=1

DC Code §2-1931
http://weblinks.westlaw.com/Find/default.wl?CFID=0&DB=DC%2DST%2DTOC%3BSTADCTOC&DocName=DCCODES2%2D1931&FindType=W&fn=%5Ftop&n=1&rs=WEBL6%2E11&spa=dcc%2D1000&trailtype=26&vr=2%2E0&Action=DODIS&CanDisNum=1

Attachment J.19
Performance Based Incentive System Scoring Algorithm

The District's performance based incentives program is designed to motivate health plans to meet and exceed performance benchmarks on quality of care, access-to-care and administrative functions, as well as patient satisfaction. Performance bonuses will be awarded on the basis of a Contractor's cumulative points (described below) and its relative proportion of Enrollees. Rewards for performance on Enrollee satisfaction will be based on cumulative points only. Contractors (i.e., plans or health plans) shall be subject to the District's performance based incentive program and will be separately evaluated on the DCHFP and Alliance program, scored, and bonuses awarded in accordance with this Attachment.

Benchmarks

Scores for performance on clinical care, access to care and administrative functions will be based on the Contractor's most recently submitted HEDIS® data and compared to the most recent national Medicaid HEDIS® data as published by NCQA. The 50th, 75th and 90th percentiles will be used for scoring purposes and the Alliance and Medicaid programs shall be scored independently.

Scoring Methodology and Measures

For each measure of clinical performance, Contractor will receive:

- Zero (0) points if its performance is below the national 50th percentile for Medicaid;
- One (1) point if its performance is at or above the 50th percentile and below the national 75th percentile for Medicaid;
- Two (2) points if its performance is at or above the 75th percentile and below the national 90th percentile for Medicaid; or
- Four (4) points if its performance is at or above the national 90th percentile for Medicaid.
- The highest possible clinical score will be the number of measures multiplied by four (4).

The clinical measures may include but are not limited to the following HEDIS® measures:

- Screening for Cervical Cancer
- Frequency of Prenatal Care
- Comprehensive Diabetic care, including HgA1C testing, LDL-C screening, and Eye exams

- Appropriate Management of Asthma Medications, for children and for adult
- Medical Assistance with Smoking Cessation[1]
- Medical Management of Depression
- Child and adolescent immunizations

For each measure of access-to-care performance, the health plan will receive:

- Zero (0) points if its performance is below the national 50th percentile for Medicaid;
- One (1) point if its performance is at or above the 50th percentile and below the national 75th percentile for Medicaid;
- Two (2) points if its performance is at or above the 75th percentile and below the national 90th percentile for Medicaid; or
- Four (4) points if its performance is at or above the national 90th percentile for Medicaid.
- The highest possible access-to-care score will be the number of measures multiplied by four (4).

The access-to-care measures may include but are not limited to the following HEDIS® measures:

- Well child visits for zero to fifteen (0-15) months, 3rd, 4th, 5th and 6th years of life
- Adolescent well visits
- Child dental visits
- Adults have at least one (1) Ambulatory visit per year
- Timeliness of Postpartum care

For each measure of administrative performance, the health plan will receive:

- Zero (0) points if its performance is below the national 50th percentile for Medicaid;

[1] **Please Note**: This is a CAHPS® survey measure which combines Advice to Quit Smoking, Discussing Smoking Cessation medications, and Discussing Smoking Strategies as a 2-year rolling average.

- One (1) point if its performance is at or above the 50th percentile and below the national 75th percentile for Medicaid;

- Two (2) points if its performance is at or above the 75th percentile and below the national 90th percentile for Medicaid; or

- Four (4) points if its performance is at or above the national 90th percentile for Medicaid.

- The highest possible administrative score will be the number of measures multiplied by four (4).

The administrative measures may include but are not limited to the following health plan descriptive data:

- Board Certification

Patient Satisfaction scores will be based on the health plan's most recent Adult and Child CAHPS® results. Scoring is based on the plan score (statistically significant difference) as compared with the all-plan average. For each patient satisfaction measure, the health plan will receive:

- Zero (0) points if its performance is statistically below the all-plan average;

- Two (2) points if its score is not statistically different from the all-plan average; or

- Five (5) points if its performance is statistically above the all-plan average.

The patient satisfaction measures may include but are not limited to:

- Problem Getting Needed Care for Adults and for Children

- Satisfaction with Specialty care for Adults and for Children

Performance Awards Calculations

The financial performance awards available for a given year will be distributed based on the cumulative points earned on each of four (4) domains: clinical, access-to-care, administration, and patient satisfaction. The percentage of total performance points earned in each domain will equal the percentage of total financial award that will be distributed across participating plans. For example, if the cumulative points available across clinical measures represent forty-five percent (45%) of total performance points, then forty-five percent (45%) of the award money will be distributed on the basis of weighted clinical scores. Likewise, if the maximum cumulative score for access-to-care measures is twenty-five percent (25%) of the total possible performance points, then twenty-five percent (25%) of the award money will be distributed on the basis of the weighted access-to-care scores. Thus, there are a total of four (4) domains in which plans will compete, based on performance scores.

Each plan's score and financial award received for one (1) set of measures is independent of the outcomes on the other measures. However, the actual amount of award money that a plan receives for performance in any of the four domains will be relative to the score and membership size of each competing plan. One hundred percent (100%) of the award funds in each category will be distributed.

The clinical, access-to-care, and administrative scores will be weighted by plan size in the following way. First, each plan's annual Member Months from the previous year will be divided by the total annual Member Months among all plans to determine the percentage of enrolled Medicaid Member Months assigned to that plan. For each plan, the total points earned for clinical, access-to-care and administrative performance will each separately be multiplied by the plan's percentage of member months (multiplied by one hundred (100)). This product is the plan's weighted score for each of these performance areas.

The total financial award assigned to each category will be divided by the sum of all the plans' weighted points for each category. This value is the dollar per point multiplier for each category of measures. The resulting value for each category is multiplied by the plan's weighted score for that category of performance. This product is the sum of money the plan will be awarded for that specific performance area.

The Patient Satisfaction award is calculated by dividing the dollar amount assigned to this performance area by the total (unweighted) points earned in this category for all participating plans. This value is the dollar amount per point multiplier. Each plan's points are multiplied by this value to determine the total dollar amount awarded to each plan.

The financial award for each health plan in all four performance areas are added and results in the total amount of each plan's annual financial performance award.

Funding the Performance Awards Pool

MAA, at its sole discretion, will determine a percentage of health plan capitation to withhold in order to generate the pool available for funding an annual distribution of performance awards. One hundred percent of funds collected in a given year will be distributed to participating plans in the following year, based on health plan performance, as described above. In the first year of the Performance Incentive program, health plans will be scored but incentives will be not awarded. In Year Two of the Contract, health plans will be scored. MAA will distribute performance bonus awards based on plan performance no earlier than Option Year Two of the Contract.

UNITY HEALTH CARE PHARMAC

ADDRESSES, HOURS AND TELEPHONE NUMBERS

ANACOSTIA CHC PHARMACY
1328 W Street, SE
Washington DC, 20020
Hours: 8:15 AM to 4:45 PM (Tues, Thurs & Fri)
8:15 AM to 8:00 PM (Mon, Wed,)
10:00 AM to 4:00 PM (Sat)
Tel: (202) 610-7188
Fax: (202) 610-0832
Pharmacist: Enoh Umoren

CONGRESS HEIGHTS CHC PHARMACY
3720 Martin Luther King Jr. Ave
Washington DC, 20032
Hours: 8:15 AM to 4:45 PM
Tel: (202) 279-1825
(202) 561-4248
Fax: (202) 645-0294
Pharmacist: Rahel Mersha

HUNT PLACE CHC PHARMACY
4130 Hunt Place, NE
Washington DC, 20019
Hours: 8:15 AM to 4:45 PM
Tel: (202) 388-8385
Fax: (202) 396-4941
Pharmacist: Ifeoma Offodile

WALKER JONES CHC PHARMACY
1100 First Street, NW
Washington DC, 20001
Hours: 8:15 AM to 4:45 PM (Mon to Fri)
Tel: (202) 354-1140 /41
Tel: (202) 354-1140 /41
Fax: (202) 354-1151
Pharmacists: Robert Mark
Patience Tangham

SOUTHWEST CHC PHARMACY
850 Delaware Ave SW.
Washington DC, 20024
Hours: 8:15 AM to 4:45 PM
Tel: (202) 548-4548
Fax: (202) 554-0459
Pharmacist: Evelyn Molen

UNITY HEALTH CARE PHARMACY AT DC GENERAL
1900 Massachusetts Ave, SE
Washington DC, 20003
Hours: 10:00 AM to 6:30 PM (Mon-Fri)
10:00 AM to 4:00 PM (Sat.)
Tel: (202) 548-6565
Fax: (202) 548-6570
Pharmacists: Ronald Norvell
Muyideen Okanlawon

UPPER CARDOZO CHC PHARMACY
3020 14TH ST. NW.
Washington DC, 2000
Hours: 8:00 AM to 8:30PM (Mon & Wed)
8:00 AM to 5:30 PM (Tues, Thur, Fri)
8:00 AM to 2:30 PM (Sat)
Tel: (202) 518-6417
(202) 518-6414
Fax: (202) 745-0194
Pharmacists: Adenike Akingbe
Ralph Dove

St. Elizabeth Pharmacy
Jerome Booker ; Pharmacy Technician
Tel: (202) 645-9850
Fax: (202) 645-0924

Assistant Direct or of Pharmacy
Alexander McLaughlin
Tel: (202) 548-6565
Cell: (202) 210-5358

Director of Pharmacy: Roderick Nwokorie
Office: (202) 548-2363; Cell: (202) 549-3404; Fax: (202) 548-2362

DISTRICT OF COLUMBIA HEALTH CARE ALLIANCE

DRUG FORMULARY

2006-2007

TABLE OF CONTENTS

USE OF THE FORMULARY……. 2
PHARMACY BENEFIT……... 3
PHARMACY, AND THERAPEUTICS COMMITTEE……..... 4
Formulary Additions and Deletions…….. 4
Generic Substitutions…… 4
Formulary Status…….…….. 4
PHARMACY LOCATIONS……..……. 5
THERAPEUTIC CATEGORY LISTING OF DRUGS…….…. 6
ALPHABETICAL LISTING OF DRUGS BY GENERIC NAME…… 29
ALPHABETICAL LISTING OF DRUGS BY BRAND NAME…… 39
APPENDIX…….. 49
AIDS DRUG ASSISTANCE PROGRAM FORMULARY……. 50
POUND-KILOGRAM CONVERSIONS……. 51
PHARMACOKINETIC FORMULAS……. 52
A. Ideal Body Weight……... 52
B. Creatinine Clearance (CrCl)……. 52
C. Creatinine Clearance Values In Renal Dysfunction……. 53
D. Body Surface Area……... 53
TEMPERATURE CONVERSION……... 53
GLUCOCORTICOID EQUIVALENCIES, POTENCIES, & HALF-LIFE …… 53
APPROXIMATE DOSAGE EQUIVALENTS OF THYROID PRODUCTS……. 54
NARCOTIC AGONISTS (COMPARATIVE PHARMACOKINETICS) ……... 54
GUIDELINE FOR DRUG LEVELS COMMONLY MONITORED…….. 55
ADJUSTMENT OF SERUM CONC. WITH LOW SERUM ALBUMIN…….. 56
DRUGS WHICH MAY CAUSE DISCOLORATION OF THE FECES……. 56
DRUGS WHICH MAY CAUSE DISCOLORATION OF URINE……. 57
DRUGS WHICH AFFECT LABORATORY VALUES…….. 58
REQUEST FOR FORMULARY CHANGE …… 61

USE OF FORMULARY

The District of Columbia Health Care Alliance formulary is divided into five sections.

The **first section** is a compilation of selected policies, guidelines, medical and pharmaceutical information designed to assist the practitioner in the care of patients.

The **second section** is a drug listing within therapeutic category and subcategory as classified by American Hospital Formulary Service. Medications are listed by generic name with a cross-reference to its common trade name. The inclusion of a trade name is for information and cross-referencing only and does not necessarily coincide with the product currently stocked.

The **third section** is a listing of all medication alphabetized generically with cross-referencing to brand names.

The **fourth section** is a listing of all medication alphabetized by brand name with cross-referencing to generic names.

The **fifth section**, the Appendix, is a compilation of tables, guidelines, and information, which can be very useful in consideration of patient care. **(Contains ADAP Formulary)**

PRESCRIPTION PLAN SUMMARY

Description of Benefits	**Coverage**
Deductible	None
Co-Pay	None
Generic Mandate	Generic equivalents may be substituted for products considered identical with respect to active components, therapeutic effectiveness, and bioavailability.
Quantity Limits	Maximum thirty day supply
Refill Limits	No sooner than the date when at least 75% of your prescription should have been used (If a 30 day supply was issued, a prescription may be refilled after day 23). Prescriptions are valid for a maximum of 12 months.

Alliance Pharmacies will only stock formulary medication

The Alliance Formulary may not totally eliminate the need to participate in compassionate use programs or other public or privately funded medication access programs.

The program does not cover Antiretrovirals. Alliance patients are eligible to participate in the AIDS Drug Assistance Program (ADAP). ADAP currently carries every commercially available antiretroviral. (The ADAP Formulary is included for reference in the Appendix – Fifth Section).

Non-formulary psychotropic drugs should be available through the Department of Mental Health.

PHARMACY AND THERAPEUTICS COMMITTEE

The primary purpose of the committee is to develop a system whereby medications are evaluated, appraised and selected such that drugs considered most useful for patient care are on the Alliance Drug Formulary. It reviews request for formulary change and prevents unnecessary duplication of the same basic drug or its combination. Evaluates the formulary and provides for its constant revision to accommodate changing needs and advances in therapeutics. Studies problems involved in the prescribing, distribution, administration, monitoring and labeling of medication. Assesses the Health Care Alliance's entire medication use system for the purpose of assuring rational prescribing, appropriate use, safety, and cost effectiveness.

FORMULARY ADDITIONS AND DELETIONS

The Pharmacy and Therapeutics Committee (P&T) makes recommendations for formulary changes. Final approval authority rests with the Department of Health. The P&T Committee utilizes a class review process to evaluate the formulary. Formulary reviews take into consideration the following criteria: the client population served, effectiveness, risk and cost.

In addition to the class review process any Alliance physician may petition the committee in writing to review a drug for formulary inclusion. The request should address the advantages of the new agent or the unmet need. Individual request should be made utilizing the Request for Formulary Change Form; a copy of the form is located in the appendix section of this manual. It may be photo copied and utilized as an official request form.

In addition to the above processes, formulary deletion request will be initiated by the pharmaceutical service department based on trends in product use.

GENERIC SUBSTITUTIONS

The Pharmacy and Therapeutics Committee has approved the dispensing of generic equivalents. Generic equivalents are drug products considered identical with respect to active component, therapeutic effectiveness, and bioavailability.

FORMULARY STATUS

Formulary Drug: A drug approved by the committee for inclusion on the Alliance formulary. Formulary drugs are generally available for routine use.

Restricted Drug: A drug approved by the committee for inclusion on the Alliance formulary, however, prescribing of this drug will be limited in scope (i.e., to a particular physician, medical service or protocol).

Nonformulary Drug: Any drug that has not been reviewed by the committee or has been reviewed and denied inclusion on the formulary. Non-formulary drugs are not stocked in Alliance Pharmacies and are not available for routine use.

PHARMACEUTICAL SERVICES

The primary responsibilities of the District of Columbia Health Care Alliance Pharmacies are to provide efficient, effective, control and distribution of pharmaceuticals to alliance patients and to provide drug information, pharmaceutical care, and comprehensive clinical pharmacy services to alliance patients, physicians, and staff.

LOCATIONS:

ANACOSTIA CLINIC
1328 W. St., S.E.
Washington, D.C. 20020
Phone (202) 610-7188
Fax (202) 610-0832

DC GENERAL PHARMACY
19th St & Mass Ave S.E.
Washington, D.C. 20003
Phone (202) 548-6565
Fax (202) 548-6570

SOUTHWEST CLINIC
850 Delaware Ave., S.W.
Washington D.C. 20024
Phone (202) 548-4548
Fax (202) 314-0997

CONGRESS HEIGHT CLINIC
3720 MLK JR, Ave., SE
Washington, D.C. 20032
Phone (202) 561-4248
Fax (202) 645-6517

HUNT PLACE CLINIC
4130 Hunt Place, N.E.
Washington, D.C. 20019
Phone (202) 388-8385
Fax (202) 727-5009

UPPER CARDOZO CLINIC
3020 14TH St., N.W.
Washington, D.C. 20009
Phone (202) 518-6417
Fax (202) 745-0194

WALKER JONES CLINIC
1100 First St., N.W.
Washington, D.C. 20001
Phone (202) 354-1141
Fax (202) 354-1151

THERAPEUTIC CATEGORY INDEX

I. ANTIHISTAMINE ……..……... 10

II. ANTI-INFECTIVE AGENTS…….…… 10

A. ANTIFUNGAL ANTIBIOTICS ……. …….……. 10
B. ANTIHELMINTICS ……..... 10
C. ANTIMALARIAL AGENTS…….…… 11
D. ANTITUBERCULOSIS AGENTS…… 11
E. ANTIVIRALS…… 11
F. CEPHALOSPORINS……. 10
G. MACROLIDE ANTIBIOTICS…….…. 10
H. MISC ANTIBIOTICS…….……... 11
I. MISC ANTI-INFECTIVES…….…….. 12
J. PENICILLINS…….……... 10/11
K. QUINOLONES…….……. 12
L. SULFONAMIDES…….…… 12
M. SULFONES…….…….. 12
N. TETRACYCLINES…….……... 11
O. URINARY ANTI-INFECTIVES……..……... 12

III. ANTINEOPLASTIC AGENTS…….……. 12

IV. AUTONOMIC DRUGS…….……. 13

A. ANTIMUSCARINICS/ANTISPASMODICS……... 13
B. ANTIPARKINSONIAN AGENTS……. 13
C. PARASYMPATHOMIMETIC (CHOLINERGIC AGENTS)……... 13
D. SKELETAL MUSCLE RELAXANTS……... 14
E. SYMPATHOLYTIC (ADRENERGIC BLOCKING) AGENTS…….. 14
F. SYMPATHOMIMETIC (ADRENERGIC) AGENTS…..……..... 13

V. BLOOD FORMATION AND COAGULATION……. 14

A. ANTICOAGULANTS…….…….….. 14
B. HEMORHEOLOGIC AGENTS……. 14
C. IRON PREPARATION…….……. 14

VI. CARDIOVASCULAR DRUGS ……...…….….… 14

A. ANTILIPEMIC AGENTS…….……. 15
B. CARDIAC DRUGS…….……... 14/15
C. HYPOTENSIVE AGENTS…….…… 15/16
D. VASODILATING AGENTS……..…….…… 16

VII. CENTRAL NERVOUS SYSTEM DRUGS……..……..… 16

A. ANTIDEPRESSANTS…….……..… 18
B. ANTIMANIC AGENTS……..…….…….…. 19
C. ANTIPSYCHOTIC AGENTS……..…….….… 18
D. BARBITURATES……..….…….……... 17/18
E. BENZODIAZEPINES……..…….…….…… 17/19
F. HYDANTOINS…….…..…….……... 16
G. MISC ANALGESICS AND ANTIPYRETICS……..…….……... 17
H. MISC ANTICONVULSANTS……..…….…… 17
I. MISC ANXIOLYTICS, SEDATINES AND HYPNOTICS……..…….……... 19
J. MISC CENTRAL NERVOUS SYSTEM AGENTS……..…….…….. 19
K. NONSTEROIDAL ANTI -INFLAMMATORY AGENTS……..….…… 16
L. OPIATE AGONISTS…….……. 16/17
M. RESPIRATORY AND CEREBRAL STIMULANTS ……..…… 18

VIII. CONTRACEPTIVES (e.g. FOAMS, DEVICES)……...……. 19

IX. DIAGNOSTIC AGENTS……...…….……. 19

A. ROENTGENOGRAPHY……...…….…… 19

X. ELECTROLYTIC CALORIC AND WATER BALANCE……..…….. 20

A. ALKALINIZING AGENTS……..…….…… 20
B. AMMONIA DETOXICANTS ……..….…… 20
C. DIURETICS…….……...…….... 20
D. POTASSIUM -REMOVING RESINS……..…..…… 20
E. POTASSIUM – SPARING DIURETICS……... 20
F. REPLACEMENT SOLUTIONS……...…..…… 20
G. URICOSURIC AGENTS……...…….…… 21

XI. ENZYMES…….…….……...…….. 21

XII. ANTITUSSIVES, EXPECTORANTS AND MUCYOLYTIC……...…… 21

A. ANTITUSSIVES…….…...……. 21
B. EXPECTORANTS…….……...…….. 21

XIII. EYE, EAR, NOSE AND THROAT (EENT) PREPARATIONS…….…...…… 21

A. ANTIBIOTICS…….……...……... 21
B ANTI-INFLAMMATORY AGENTS……. 22
C ANTIVIRALS…….……...……. 21
D. CARBONIC ANHYDRASE INHIBITORS……...…… 22
E. LOCAL ANESTHETICS……...…… 22
F. MISC EENT DRUG…….……...…… 23

G. MISC ANTI -INFECTIVES……...…..... 22
H. MIOTICS…….……...…… 22
I. MOUTHWASHES AND GARGLES……...…….. 22
J. MYDRIATICS…….…….…..…..... 22
K. SULFONAMIDES…….……...…….. 21
L. VASOCONSTRICTORS…… 23

XIV. GASTROINTESTINAL DRUGS…… 23

A. ANTACIDS AND ADSORBENTS……...……. 23
B. ANTIDIARRHEAL AGENTS……..…….… 23
C. ANTIEMETICS…….……...…….. 23/24
D. CATHARTICS AND LAXATIVES……...…… 23
E. DIGESTANTS…….……...……..... 23
F. MISC GI DRUGS……....……... 24

XV. GOLD COMPOUNDS…….…… 24

XVI. HEAVY METAL ANTAGONISTS……...…….… 24

XVII. HORMONES AND SYNTHETIC SUBSTITUTES……...…… 24

A. ADRENALS…….…….….. 24
B. ANTITHYROID AGENTS…….…… 26
C. CONTRACEPTIVES…….……. 24/25
D. ESTROGENS…….…….… 25
E. INSULINS…….…….……. 25
F. MISC ANTIDIABETIC AGENTS……. 25
G. PROGESTINS…….…… 25
H. SULFONYL UREAS…….……. 25
I. THYROID AGENTS…….. 25/26

XVIII. OXYTOCICS…….……...….…….. 26

XIX. SKIN AND MUCCOUS MEMBRANE AGENTS…….. 26

A. ANTIBIOTICS.…….…….. 26
B. ANTIFUNGALS…….…… 26
C. ANTI-INFLAMMATORY AGENTS……. 27
D. ANTI -PRURITICS AND LOCAL ANESTHETICS …… 27
E. ANTIVIRALS.…….……... 26
F. KERATOLYTIC AGENTS……...…….… 27
G. KERATOPLASTIC AGENTS…… 27
H. MISC LOCAL ANTI –INFECTIVES……...……. 27
I. MISC SKIN AND MUCOUS MEMBRANE AGENTS.……...…… 27
J. SCABICIDES AND PEDICULICIDES……...…….. 26

XX. SMOOTH MUSCLE RELAXANTS……...…… 27

A. GENITOURINARY SMOOTH MUSCLE RELAXANTS……...……. 27
B. RESPIRATORY SMOOTH MUSCLE RELAXANTS…….. 28

XXI VITAMINS…….…...……... 28

A. MULTIVITAMIN PREPARATIONS.……...…… 28
B. VITAMIN B COMPLEX…….……... 28
C. VITAMIN D…….……... 28
D. VITAMIN K ACTIVITY…….….…….. 28

XXII. UNCLASSIFIED THERAPEUTIC AGENTS.…… 28

XXIII. DEVICES…….…….……... 28

DRUG LISTING BY GENERIC NAME
WITHIN CATEGORY AND SUBCATEGORY

Generic Name	Trade Name

Category: ANTIHISTAMINE DRUGS

LORATADINE 10MG TAB	CLARITIN 10MG TAB
LORATADINE 5MG/5ML SYRUP	CLARITIN 5MG/5ML SYRUP
DIPHENHYDRAMINE 12.5MG/5ML ELX	BENADRYL 12.5MG/5ML ELXIR
DIPHENHYDRAMINE 25MG CAPS	BENADRYL 25MG CAP
PROMETHAZINE HCL 25MG SUPP	PHENERGAN 25MG SUPP
PROMETHAZINE HCL 50MG SUPP	PHENERGAN 50MG SUPP

Category: ANTI-INFECTIVE AGENTS
Subcategory: Anthelmintics

MEBENDAZOLE 100MG CHEWABLE TAB	VERMOX 100MG CHEWABLE TAB

Subcategory: Antibiotics
Subcategory: Antifungal Antibiotics

FLUCONAZOLE 150MG TAB	DIFLUCAN 150MG TAB
GRISEOFULVIN 125MG/5ML SUSP	GRIFULVIN V 125MG/5ML SUSP
GRISEOFULVIN 250MG TAB	GRIFULVIN V 250MG TAB
NYSTATIN 100000U/ML SUSP	NILSTAT 100000U/ML SUSP

Subcategory: Cephalosporins

CEPHALEXIN 125MG/5ML ORAL SUSP	KEFLEX 125MG/5ML ORAL SUSP
CEPHALEXIN 250MG CAP	KEFLEX 250MG CAP
CEPHALEXIN 500MG CAP	KEFLEX 500MG CAP

Subcategory: Macrolide Antibiotics

AZITHROMYCIN 250MG CAP (Z-PAK)	ZITHROMAX 250MG CAP (Z-PAK)
AZITHROMYCIN 600MG/15ML SUSP	ZITHROMAX 600MG/15ML ORAL SUSP
AZITHROMYCIN 900MG/22.5ML SUSP	ZITHROMAX 900MG/22.5ML SUSP
CLARITHROMYCIN 250MG TAB	BIAXIN 250MG TAB
CLARITHROMYCIN 500MG TAB	BIAXIN 500MG TAB
ERYTHROMYCIN 200MG/5ML SUSP	E.E.S. 200MG/5ML SUSP
ERYTHROMYCIN 250MG FILMTAB	E.E.S 250MG FILMTAB

Subcategory: Penicillins

AMOXICILLIN 125/CLAV 31.25/5ML	AUGMENTIN 125 SUSP
AMOXICILLIN 125MG/5ML SUSP	TRIMOX 125/5ML SUSP

Generic Name	Trade Name
AMOXICILLIN 250/CLAV 125 TAB	AUGMENTIN 250MG TAB
AMOXICILLIN 250/CLAV 62.5/5ML	AUGMENTIN 250 SUSP
AMOXICILLIN 250MG CAP	AMOXICILLIN 250MG CAP
AMOXICILLIN 250MG/5ML SUSP	TRIMOX 250MG/5ML SUSP
AMOXICILLIN 500/CLAV 125 TAB	AUGMENTIN 500MG TAB
AMOXICILLIN 500MG CAP	AMOXICILLIN 500MG CAP
AMOXICILLIN 875/CLAV 125 TAB	AUGMENTIN 875MG TAB
DICLOXACILLIN 250MG CAP	PATHOCIL 250MG CAP
PENICILLIN VK 250MG TAB	PENICILLIN VK 250MG TAB
PENICILLIN VK 250MG/5ML SUSP	LEDERCILLIN VK 250MG/5ML SUSP

Subcategory: Tetracyclines

DOXYCYCLINE 100MG CAP	VIBRAMYCIN 100MG CAP
TETRACYCLINE 250MG CAP	SUMYCIN 250MG CAP

Subcategory: Misc Antibiotics

CLINDAMYCIN 150MG CAP	CLEOCIN 150MG CAP

Subcategory: Antituberculosis Agents

ETHAMBUTOL 100MG TAB	MYAMBUTOL 100MG TAB
ETHAMBUTOL 400MG TAB	MYAMBUTOL 400MG TAB
ISONIAZID 100MG TAB	ISONIAZID 100MG TAB
ISONIAZID 300MG TAB	ISONIAZID 300MG TAB
ISONIAZID 50MG/5ML SYRUP	ISONIAZID 50MG/5ML SYRUP
PYRAZINAMIDE 500MG TAB	PYRAZINAMIDE 500MG TAB
RIFAMPIN 300MG CAP	RIMACTANE 300MG CAP

Subcategory: Antivirals

ACYCLOVIR 200MG CAP	ZOVIRAX 200MG CAP

Subcategory: Antimalarial Agents

HYDROXYCHLOROQUINE 200MG TAB	PLAQUENIL 200MG TAB
PRIMAQUINE 26.3MG TAB	PRIMAQUINE 26.3MG TAB
PYRIMETHAMINE 25MG TAB	DARAPRIM 25MG TAB

Generic Name	Trade Name

Subcategory: Quinolones

CIPROFLOXACIN HCL 250MG TAB	CIPRO 250MG TAB
CIPROFLOXACIN HCL 500MG TAB	CIPRO 500MG TAB
CIPROFLOXACIN HCL 750MG TAB	CIPRO 750MG TAB
LEVOFLOXACIN 250MG TAB	LEVAQUIN 250MG TAB
LEVOFLOXACIN 500MG TAB	LEVAQUIN 500MG TAB
LEVOFLOXACIN 750MG TAB	LEVAQUIN 750MG TAB

Subcategory: Sulfonamides

ERYTHROMYCIN/SULFISOX ORL SUSP	PEDIAZOLE ORAL SUSP
SULFADIAZINE 500MG TAB	SULFADIAZINE 500MG TAB
SULFASALAZINE 500MG TAB	AZULFIDINE 500MG TAB

Subcategory: Sulfones

DAPSONE 100MG TAB	DAPSONE 100MG TAB
DAPSONE 25MG TAB	DAPSONE 25MG TAB

Subcategory: Urinary Anti-Infectives

NITROFURANTOIN 100MG CAP	MACRODANTIN 100MG CAP
NITROFURANTOIN 50MG CAP	MACRODANTIN 50MG CAP
TRIMETHOPRIM 100MG TAB	TRIMPEX 100MG TAB

Subcategory: Misc Anti-Infectives

METRONIDAZOLE 250MG TAB	FLAGYL 250MG TAB
SULFAMETH 200/TRIMETH 40MG/5ML	BACTRIM PEDIATRIC ORAL SUSP
SULFAMETH 800/TRIMET l60MG TAB	BACTRIM DS TAB

Category: ANTINEOPLASTIC AGENTS

BUSULFAN 2MG TAB	MYLERAN 2MG TAB
CHLORAMBUCIL 2MG TAB	LEUKERAN 2MG TAB
HYDROXYUREA 500MG CAP	HYDREA 500MG CAP
MEGESTROL 40MG TAB	MEGACE 40MG TAB
MEGESTROL 40MG/ML ORAL SUSP	MEGACE 40MG/ML ORAL SUSP
MELPHALAN 2MG TAB	ALKERAN 2MG TAB
METHOTREXATE 2.5MG TAB	METHOTREXATE 2.5MG TAB
TAMOXIFEN 10MG TAB	NOLVADEX 10MG TAB

Generic Name	Trade Name

Category: AUTONOMIC DRUGS
Subcategory: Parasympathomimetic (Cholinergic Agents)

BETHANECHOL 25MG TAB	URECHOLINE 25MG TAB
BETHANECHOL 5MG TAB	URECHOLINE 5MG TAB
BETHANECOL 10MG TAB	URECHOLINE 10MG TAB
PYRIDOSTIGMINE 60MG TAB	MESTINON 60MG TAB

Subcategory: Anticholinergic Agents
Subcategory: Antiparkinsonian Agents

BENZTROPINE 1MG TAB	COGENTIN 1MG TAB
BENZTROPINE 2MG TAB	COGENTIN 2MG TAB

Subcategory: Antimuscarinics/Antispasmodics

DICYCLOMINE 10MG CAP	BENTYL 10MG CAP
IPRATROPIUM BR INHALER	ATROVENT INHALER
PROPANTHELINE 15MG TAB	PROBANTHINE 15MG TAB

Subcategory: Sympathomimetic (Adrenergic) Agents

ALBUTEROL 2MG TAB	PROVENTIL 2MG TAB
ALBUTEROL 2MG/5ML SYRUP	PROVENTIL 2MG/5ML SYRUP
ALBUTEROL 4MG REPETAB	PROVENTIL 4MG REPETAB
ALBUTEROL 4MG TAB	PROVENTIL 4MG TAB
ALBUTEROL METERED INHALER	PROVENTIL METERED INHALER
ALBUTEROL 0.083% NEB UD SOL	PROVENTIL 0.083% NEB UD SOL
ALBUTEROL/IPRATROPIUM INHALER	COMBIVENT INHALER
METAPROTERENOL 10MG TAB	ALUPENT 10MG TAB
METAPROTERENOL 5% INH SOLUTION	ALUPENT 5% INH SOLUTION
METAPROTERENOL METERED INHALER	ALUPENT METERED INHALER
SALMETRL-FLUTICASON 100/50 DISK	ADVAIR 100/50MCG DISK INH
SALMETRL-FLUTICASON 250/50 DISK	ADVAIR 250/50MCG DISKUS INH
SALMETRL-FLUTICASON 500/50 DISK	ADVAIR 500/50MCG DISKUS INH
SALMETEROL XINAFOATE DISKUS INH	SEREVENT DISKUS 50MCG INH
TERBUTALINE 2.5MG TAB	BRETHINE 2.5MG TAB
TERBUTALINE 5MG TAB	BRETHINE 5MG TAB

Generic Name	Trade Name

Subcategory: Sympatholytic (Adrenergic Blocking) Agents

ERGOTAMINE 1MG/CAFF 100MG TAB	CAFERGOT TABLET

Subcategory: Skeletal Muscle Relaxants

BACLOFEN 10MG TAB	LIORESAL 10MG TAB
CYCLOBENZAPRINE 10MG TAB	FLEXERIL 10MG TAB

Category: BLOOD FORMATION AND COAGULATION
Subcategory: Antianemia Drugs
Subcategory: Iron Preparations

FERROUS SULF 325MG TAB UD	FERROUS SULF 325MG TAB UD
FERROUS SULF 220MG/5ML ELIXIR	FERROUS SULF 220/5ML ELIXIR

Subcategory: Coagulants and Anticoagulants
Subcategory: Anticoagulants

WARFARIN SODIUM 5MG TAB	COUMADIN 5MG TAB
WARFARIN SODIUM 2.5MG TAB	COUMADIN 2.5MG TAB

Subcategory: Hemorrheologic Agents

PENTOXIFYLLINE 400MG TAB SA	TRENTAL 400MG TAB SA

Category: CAROIOVASCULAR DRUGS
Subcategory: Cardiac Drugs

AMIODARONE 200MG TAB	CORDARONE 200MG TAB
AMLODIPINE BESYLATE 10MG TAB	NORVASC 10MG TAB
AMLODIPINE BESYLATE 5MG TAB	NORVASC 5MG TAB
ATENOLOL 50MG TAB	TENORMIN 50MG TAB
CAPTOPRIL 12.5MG TAB	CAPOTEN 12.5MG TAB
CAPTOPRIL 25MG TAB	CAPOTEN 25MG TAB
DIGOXIN 0.05MG/ML ELIXIR	LANOXIN 0.05MG/ML ELIXIR
DIGOXIN 0.125MG TAB	LANOXIN 0.125MG TAB
DIGOXIN 0.25MG TAB	LANOXIN 0.25MG TAB
DILTIAZEM 180MG CR CAP	TIAZAC 180MG CR CAP
DILTIAZEM 30MG TAB	CARDIZEM 30MG TAB
DILTIAZEM 60MG TAB	CARDIZEM 60MG TAB
DILTIAZEM HCL 240MG CR CAP	TIAZAC 240MG CR CAP
DILTIAZEM HCL 300MG CR CAP	TIAZAC 300MG CR CAP
FOSINOPRIL SODIUM 10MG TAB	MONOPRIL 10MG TAB
FOSINOPRIL SODIUM 20MG TAB	MONOPRIL 20MG TAB

Generic Name	Trade Name
FOSINOPRIL SODIUM 40MG TAB	MONOPRIL 40MG TAB
LISINOPRIL 10MG TAB	ZESTRIL 10MG TAB
LISINOPRIL 20MG TAB	ZESTRIL 20MG TAB
LISINOPRIL 5MG TAB	ZESTRIL 5MG TAB
METOPROLOL 50MG TAB	LOPRESSOR 50MG TAB
NIFEDIPINE 10MG CAP	PROCARDIA 10MG CAP
NIFEDIPINE CC 30MG TAB	ADALAT CC 30MG TAB
NIFEDIPINE CC 60MG TAB	ADALAT CC 60MG TAB
NIFEDIPINE CC 90MG TAB	ADALAT CC 90MG TAB
PROCAINAMIDE 250MG CAP	PROCAN 250MG CAP
PROCAINAMIDE SR 500MG TAB	PROCAN SR 500MG TAB
PROPRANOLOL 10MG TAB	INDERAL 10MG TAB
PROPRANOLOL 40MG TAB	INDERAL 40MG TAB
PROPRANOLOL LA l20MG CAP	INDERAL LA l20MG CAP
PROPRANOLOL LA l60MG CAP	INDERAL LA l60MG CAP
PROPRANOLOL LA 80MG CAP	INDERAL LA 80MG CAP
QUINIDINE GLUCONATE 324MG TAB	QUINAGLUTE 324MG TAB
QUINIDINE SULFATE 200MG TAB	QUINORA 200MG TAB
VERAPAMIL l20MG TAB	CALAN l20MG TAB
VERAPAMIL 240MG CAP SA	VERELAN 240MG CAP SA
VERAPAMIL 80MG TAB	CALAN 80MG TAB

Subcategory: Antilipemic Agents

ATORVASTATIN 80MG TAB	LIPITOR 80MG TAB
CHOLESTYRAMINE LIGHT PKT	QUESTRAN LIGHT PKT
SIMVASTATIN 5MG TAB	ZOCOR 5MG TAB
SIMVASTATIN 10MG TAB	ZOCOR 10MG TAB
SIMVASTATIN 20MG TAB	ZOCOR 20MG TAB
SIMVASTATIN 40MG TAB	ZOCOR 40MG TAB
SIMVASTATIN 80MG TAB	ZOCOR 80MG TAB

Subcategory: Hypotensive Agents

CLONIDINE HCL 0.1MG TAB	CATAPRES 0.1MG TAB
CLONIDINE HCL 0.2MG TAB	CATAPRES 0.2MG TAB
CLONIDINE HCL 0.3MG TAB	CATAPRES 0.3MG TAB
CLONIDINE-TTS 1 PATCH	CATAPRES-TTS 1 PATCH
CLONIDINE-TTS 2 PATCH	CATAPRES-TTS 2 PATCH
CLONIDINE-TTS 3 PATCH	CATAPRES-TTS 3 PATCH
DOXAZOSIN MESYLATE 1MG TAB	CARDURA 1MG TAB
DOXAZOSIN MESYLATE 2MG TAB	CARDURA 2MG TAB
DOXAZOSIN MESYLATE 4MG TAB	CARDURA 4MG TAB
HYDRALAZINE 25MG TAB	APRESOLINE 25MG TAB
HYDRALAZINE 50MG TAB	APRESOLINE 50MG TAB
LABETALOL 100MG TAB	NORMODYNE 100MG TAB

Generic Name	Trade Name
LABETALOL 200MG TAB	NORMODYNE 200MG TAB
METHYLDOPA 250MG TAB	ALDOMET 250MG TAB
MINOXIDIL 10MG TAB	LONITEN 10MG TAB
MINOXIDIL 2.5MG TAB	LONITEN 2.5MG TAB
TELMISARTAN 40MG TAB	MICARDIS 40MG TAB
TELMISARTAN 80MG TAB	MICARDIS 80MG TAB

Subcategory: Vasodilating Agents

DIPYRIDAMOLE 25MG TAB	PERSANTINE 25MG TAB
ISOSORBIDE MONONIT l20MG TB CR	IMDUR l20MG TAB CR
ISOSORBIDE MONONIT 30MG TAB CR	IMDUR 30MG TAB CR
ISOSORBIDE MONONIT 60MG TAB CR	IMDUR 60MG TAB CR
NITROGLYCERIN 0.2MG/HR PATCH	TRANSDERM-NITRO 0.2MG/HR PATCH
NITROGLYCERIN 0.4MG TAB SL	NITROSTAT 0.4MG TAB SL
NITROGLYCERIN 0.4MG/HR PATCH	NITRO-DUR 0.4MG/HR PATCH
NITROGLYCERIN 0.6MG TAB SL	NITROSTAT 0.6MG TAB SL
NITROGLYCERIN 2% OINT	NITROL 2% OINT

Category: CENTRAL NERVOUS SYSTEM DRUGS
Subcategory: Analgesics and Antipyretics
Subcategory: Nonsteroidal Anti-inflammatory Agents

BUTALB 50/CAFF 40/ASA 325 TAB	FIORINAL TAB
IBUPROFEN 400MG TAB	MOTRIN 400MG TAB
IBUPROFEN 600MG TAB	MOTRIN 600MG TAB
INDOMETHACIN 25MG CAP	INDOCIN 25MG CAP
KETOPROFEN 50MG CAP	ORUDIS 50MG CAP
NAPROXEN 250MG TAB	NAPROSYN 250MG TAB
NAPROXEN 375MG TAB	NAPROSYN 375MG TAB
PIROXICAM 10MG CAP	FELDENE 10MG CAP
PIROXICAM 20MG CAP	FELDENE 20MG CAP
SULINDAC 150MG TAB	CLINORIL 150MG TAB
SULINDAC 200MG TAB	CLINORIL 200MG TAB
TOLMETIN 400MG DS CAP	TOLECTIN DS 400MG CAP

Subcategory: Opiate Agonists

ACETAMINO 120/COD 12MG/5ML ELX	TYLENOL W/CODEINE ELIXIR
ACETAMINO 300/CODEINE 30MG TAB	TYLENOL W/ CODEINE NO.3 TAB
CODEINE SULFATE 30MG TAB	CODEINE 30MG TAB
HYDROMORPHONE 2MG TAB	DILAUDID 2MG TAB
MEPERIDINE 50MG TAB	DEMEROL 50MG TAB

Generic Name	Trade Name
MORPHINE SUL 20MG/ML-120ML SOL	ROXANOL 20MG/ML-12-ML SOL
MORPHINE SULFATE 20MG/ML SOLN	ROXANOL 20MG/ML SOLN
MORPHINE SULFATE 30MG SA TAB	MS CONTIN 30MG SA TAB
OXYCODONE 5/ACETAMIN 325MG TAB	PERCOCET 5/325MG TAB

Subcategory: Misc Analgesics and Antipyretics

ACETAMINOPHEN 100MG/ML DROP	TYLENOL 100MG/ML DROP
ACETAMINOPHEN 160MG/5ML LIQ	TYLENOL 160MG/5ML ELX

Subcategory: Anticonvulsants
Subcategory: Barbiturates

PRIMIDONE 250MG TAB	MYSOLINE 250MG TAB

Subcategory: Benzodiazepines

CLONAZEPAM 0.5MG TAB	KLONOPIN 0.5MG TAB
CLONAZEPAM 1MG TAB	KLONOPIN 1MG TAB
CLONAZEPAM 2MG TAB	KLONOPIN 2MG TAB

Subcategory: Hydantoins

PHENYTOIN 100MG CAP	DILANTIN 100MG CAP
PHENYTOIN 125MG/SML SUSP	DILANTIN 125MG/SML SUSP
PHENYTOIN 50MG TAB	DILANTIN 50MG TAB
PHENYTOIN SOD 30MG SR CAP	DILANTIN 30MG SR CAP

Subcategory: Misc Anticonvulsants

CARBAMAZEPINE 100MG TAB	TEGRETOL 100MG TAB
CARBAMAZEPINE 100MG/SML SUSP	TEGRETOL 100MG/SML SUSP
CARBAMAZEPINE 200MG TAB	TEGRETOL 200MG TAB
GABAPENTIN 300MG CAP	NEURONTIN 300MG CAP
GABAPENTIN 400MG CAP	NEURONTIN 400MG CAP
LAMOTRIGINE 100MG TAB	LAMICTAL 100MG TAB
LAMOTRIGINE 25MG TAB	LAMICTAL 25MG TAB
VALPROIC ACID 250MG CAP	DEPAKENE 250MG CAP

DRUG LISTING BY GENERIC NAME
WITHIN CATEGORY AND SUBCATEGORY

Generic Name	Trade Name
Subcategory: Psychotherapeutic Agents	
Subcategory: Antidepressants	
AMITRIPTYLINE 10MG TAB	ELAVIL 10MG TAB
AMITRIPTYLINE 25MG TAB	ELAVIL 25MG TAB
AMITRIPTYLINE HCL 50MG TAB	ELAVIL 50MG TAB
DESIPRAMINE 10MG TAB	NORPRAMIN 10MG TAB
DESIPRAMINE 25MG TAB	NORPRAMINE 25MG TAB
DESIPRAMINE 50MG TAB	NORPRAMIN 50MG TAB
IMIPRAMINE 25MG TAB	TOFRANIL 25MG TAB
IMIPRAMINE HCL 10MG TAB	TOFRANIL 10MG TAB
NORTRIPTYLINE HCL 10MG CAP	PAMELOR 10MG CAP
NORTRIPTYLINE HCL 25MG CAP	PAMELOR 25MG CAP
SERTRALINE 50MG TAB	ZOLOFT 50MG TAB
SERTRALINE HCL 100MG TAB	ZOLOFT 100MG TAB
Subcategory: Antipsychotic Agents	
CHLORPROMAZINE 25MG TAB	THORAZINE 25MG TAB
CHLORPROMAZINE 50MG TAB	THORAZINE 50MG TAB
FLUPHENAZINE 5MG TAB	PROLIXIN 5MG TAB
FLUPHENAZINE HCL 1MG TAB	PROLIXIN 1MG TAB
HALOPERIDOL 1MG TAB	HALDOL 1MG TAB
HALOPERIDOL 5MG TAB	HALDOL 5MG TAB
THIORIDAZINE 100MG TAB	MELLARIL 100MG TAB
THIORIDAZINE 25MG TAB	MELLARIL 25MG TAB
TRIFLUOPERAZINE 5MG TAB	STELAZINE 5MG TAB
Subcategory: Respiratory and Cerebral Stimulants	
METHYLPHENIDATE 10MG TAB	RITALIN 10MG TAB
Subcategory: Anxiolytics, Sedatives and Hypnotics	
Subcategory: Barbiturates	
PHENOBARBITAL 20MG/5ML EXIXIR	PHENOBARBITAL 20MG/5ML ELIXIR
PHENOBARBITAL 30MG TAB	PHENOBARBITAL 30MG TAB
Subcategory: Benzodiazepines	
ALPRAZOLAM 0.25MG TAB	XANAX 0.25MG TAB
ALPRAZOLAM 0.5MG TAB	XANAX 0.5MG TAB
ALPRAZOLAM 1MG TAB	XANAX 1MG TAB
CHLORDIAZEPOXIDE 10MG CAP	LIBRIUM 10MG CAP
CHLORDIAZEPOXIDE 25MG CAP	LIBRIUM 25MG CAP
CHLORDIAZEPOXIDE 5MG CAP	LIBRIUM 5MG CAP

Generic Name	Trade Name
DIAZEPAM 5MG TAB	VALIUM 5MG TAB
FLURAZEPAM 15MG CAP	DALMANE 15MG CAP
LORAZEPAM 0.5MG TAB	ATIVAN 0.5MG TAB
LORAZEPAM 1MG TAB	ATIVAN 1MG TAB
LORAZEPAM 2MG TAB	ATIVAN 2MG TAB

Subcategory: Misc Anxiolytics, Sedatives and Hypnotics

HYDROXYZINE 10MG/5ML SYRUP	ATARAX 10MG/5ML SYRUP
HYDROXYZINE HCL 10MG TAB	ATARAX 10MG TAB
HYDROXYZINE HCL 25MG TAB	ATARAX 25MG TAB

Subcategory: Antimanic Agents

LITHIUM CARBONATE 300MG CAP	ESKALITH 300MG CAP

Subcategory: Misc Central Nervous System Agents

CARBIDOPA/LEVODOPA-10/100 TAB	SINEMET-10/100 TABLET
CARBIDOPA/LEVADOPA-25/100 TAB	SINEMET-25/100 TABLET
CARBIDOPA/LEVADOPA-25/250 TAB	SINEMET-25/250 TABLET
SUMATRIPTAN 25MG TAB	IMITREX 25MG TAB
SUMATRIPTAN 50MG TAB	IMITREX 50MG TAB
SUMATRIPTAN 100MG TAB	IMITREX 100MG TAB

Category: CONTRACEPTIVES (e.g., Foams, Devices)

CONDOMS LUBRICATED/SPERMICIDAL	CONDOMS LUBRICATED/SPERMICIDAL
DELFEN FOAM 12.5% VAGINAL	DELFEN FOAM 12.5% VAGINAL
DIAPHRAGM ARC-SPRING 65MM	ORTHO-DIAPHRAGM ALLFLX 65MM
DIAPHRAGM ARC-SPRING 70MM	ORTHO-DIAPHRAGM ALLFLX 70MM
DIAPHRAGM ARC-SPRING 75MM	ORTHO-DIAPHRAGM ALLFLX 75MM
DIAPHRAGM ARC-SPRING 80MM	ORTHO-DIAPHRAGM ALLFLX 80MM
DIAPHRAGM ARC-SPRING 85MM	ORTHO-DIAPHRAGM ALLFLX 85MM

Category: DIAGNOSTIC AGENTS
Subcategory: Roentgenography

GASTROGRAFFIN SOLUTION	GASTROGRAFFIN SOLUTION

Generic Name	Trade Name

Category: ELECTROLYTIC CALORIC AND WATER BALANCE
Subcategory: Alkalinizing Agents

BICITRA SUGAR FREE SOLUTION	BICITRA SUGAR FREE SOLUTION

Subcategory: Ammonia Detoxicants

LACTULOSE 10GM/15ML SYRUP	CEPHULAC 10GM/15ML SYRUP

Subcategory: Replacement Solutions

CALCIUM CARBONATE 650MG TAB	CALCIUM CARBONATE 650MG TAB
POTASSIUM CHLORIDE 10% SOL	POTASSIUM CHLORIDE 10% SOL
POTASSIUM CHLORIDE 20MEQ PKT	KLOR 20MEQ PKT
POTASSIUM CHLORIDE 20MEQ TAB	KLORVESS 20MEQ TAB
POTASSIUM CL 10MEQ SA TAB	TEN-K 10MEQ SA TAB

Subcategory: Potassium-Removing Resins

SOD POLYSTYRENE SULF 15GM/60ML	SOD POLYSTYRENE SULF 15GM/60ML

Subcategory: Diuretics

BUMETANIDE 1MG TAB	BUMEX 1MG TAB
FUROSEMIDE 20MG TAB	LASIX 20MG TAB
FUROSEMIDE 40MG TAB	LASIX 40MG TAB
HYDROCHLOROTHIAZIDE 25MG TAB	ESIDREX 25MG TAB
HYDROCHLOROTHIAZIDE 50MG TAB	ESIDREX 50MG TAB
METOLAZONE 5MG TAB	DIULO 5MG TAB
TRIAMTERENE 37.5/HCTZ 25 TAB	MAXZIDE 37.5MG/25MG TAB

Subcategory: Potassium-sparing Diuretics

SPIRONOLACTONE 25MG TAB	ALDACTONE 25MG TAB
SPIRONOLACTONE/HCTZ 25/25 TAB	ALDACTAZIDE 25/25 TAB

Generic Name	Trade Name

Subcategory: Uricosuric Agents

PROBENECID 500MG TAB	BENEMID 500MG TAB

Category: ENZYMES

GRANULEX SPRAY	GRANULEX SPRAY

Category: ANTITUSSIVES, EXPECTORANTS AND MUCYOLYTIC AGENTS
Subcategory: Antitussives

GUAIFENSIN/CODEINE SYRUP	ROBITUSSIN AC SYRUP
PSEUDOEPHED/CARBINOX DM DROP	RONDEC DM DROP
PSEUDOEPHED/CARBINOX DM SYRUP	RONDEC DM SYRUP

Subcategory: Expectorants

LUGOLS SOLUTION	LUGOLS SOLUTION

Category: EYE, EAR, NOSE AND THROAT (EENT) PREPARATIONS
Subcategory: Anti-infectives
Subcategory: Antibiotics

BACITRACIN 500U/GM EYE OINT	BACITRACIN 500U/GM EYE OINT
CIPROFLOXACIN 0.3% EYE OINT	CILOXAN 0.3% EYE OINT
CIPROFLOXACIN 0.3% OPTH DROP	CILOXAN 0.3% OPTH DROP
COLY-MYCIN S OTIC DROP	COLY-MYCIN S OTIC DROP
ERYTHROMYCIN EYE OINT	ILOTYCIN EYE OINT
GENTAMICIN 3MG/ML OPTH DROP	GARAMYCIN 3MG/ML OPTH DROP
GENTAMICIN SULF EYE OINT	GARAMYCIN EYE OINT
MAXITROL OPTHALMIC DROP	MAXITROL OPTHALMIC DROP
NEOMYC/POLYM B/HC OTIC SUSP	CORTISPORIN OTIC SUSP
OFLOXACIN OTIC 0.3% DROP	FLOXIN OTIC 0.3% DROP
TOBRAMYCIN 0.3% EYE OINT	TOBREX 0.3% EYE OINT
TOBRAMYCIN 0.3% OPTH DROP	TOBREX 0.3% OPTH DROP
TOBRAMYCIN/DEXAMETHA OPTH DROP	TOBRADEX OPTH DROP
TOBRAMYCIN/DEXMETHA EYE OINT	TOBRADEX EYE OINT
TRIMETHOPRIM/POLYMIX OPTH DROP	POLYTRIM OPHTHALMIC DROP

Subcategory: Antivirals

TRIFLURIDINE 1% OPTH DROP	VIROPTIC 1% OPTH DROP

Subcategory: Sulfonamides

SULFACETAMIDE 10% OPTH DROP	SULAMYD 10% OPTH DROP

Generic Name	Trade Name
Subcategory: Misc Anti-Infectives	
ACETIC ACID 2% OTIC SOL	VOSOL 2% OTIC SOL
ACETIC ACID 2%/HC 1% OTIC SOL	VOSOL HC OTIC SOL
Subcategory: Anti-Inflammatory Agents	
FLUNISOLIDE 0.025% NASAL INH	NASALIDE 0.025% NASAL INH
FLUOROMETHOLONE EYE OINT	FML EYE OINT
KETOROLAC TROM 0.5% OPTH DROP	ACULAR 0.5% OPTH DROP
PREDNISOLONE ACET 1% OPTH DROP	PRED FORTE 1% OPTH DROP
Subcategory: Carbonic Anhydrase Inhibitors	
ACETAZOLAMIDE 250MG TAB	DIAMOX 250MG TAB
ACETAZOLAMIDE 500MG CAP SA	DIAMOX SEQUELS 500MG
DORZOLAMIDE HCL 2% OPTH DROP	TRUSOPT 2% OPTH DROP
METHAZOLAMIDE 50MG TAB	NEPTAZANE 50MG TAB
Subcategory: Local Anesthetics	
AURALGAN EAR DROP	AURALGAN EAR DROP
LIDOCAINE 2% VISCOUS SOLUTION	LIDOCAINE 2% VISCOUS SOLUTION
LIDOCAINE HCL 2% JELLY	XYL0CAINE 2% JELLY
PROPARACAINE 0.5% OPTH DROP	OPHTHETIC 0.5% OPTH DROP
Subcategory: Miotics	
PILOCARPINE 2% OPTH DROP	PILOCAR 2% OPTH DROP
PILOCARPINE 4% EYE GEL	PILOPINE HS 4% EYE GEL
PILOCARPINE 4% OPTH DROP	PILOCAR 4% OPTH DROP
Subcategory: Mydriatics	
ATROPINE 1% OPTH DROP	ATROPINE 1% OPTH DROP
CYCLOPENTOL/PHENYLEPH OPTH SOL	CYCLOMYDRIL OPTH SOLUTION
CYCLOPENTOLATE 1% OPTH DROP	CYCLOGYL 1% OPTH DROP
DIPIVEFRIN 0.1% OPTH DROP	PROPINE 0.1% OPTH DROP
HOMATROPINE 2% OPTH DROP	ISOPTO HOMATROPIN 2% OPTH DROP
HOMATROPINE 5% OPTH DROP	ISOPTO HOMATROPIN 5% OPTH DROP
SCOPOLAMINE 0.25% OPTH DROP	ISOPTO HYOSCIN 0.25% OPTH DROP
TROPICAMIDE 1% OPTH DROP	MYDRIACYL 1% OPTH DROP
Subcategory: Mouthwashes and Gargles	
MAGIC MOUTHWASH SOL	MAGIC MOUTHWASH SOL

Generic Name	Trade Name

Subcategory: Vasoconstrictors

PHENYLEPHRINE 2.5% OPTH DROP	NEOSYNEPHRINE 2.5% OPTH DROP
VASOCON-A OPHTHALMIC DROP	VASOCON-A OPHTHALMIC DROP

Subcategory: Misc EENT Drugs

BETAXOLOL HCL 0.25% OPTH DROP	BETOPTIC S 0.25% OPTH DROP
BRIMONIDINE 0.2% OPHTH DROP	ALPHAGAN 0.2% OPHTH DROP
CERUMENEX 10% EAR DROP	CERUMENEX 10% EAR DROP
HYDROXYPROPYLMETH 2.5% OPT SOL	GONIOSOL 2.5% OPTH SOLUTION
HYPOTEARS OPTH DROP	HYPOTEARS OPTH DROP
LACRILUBE EYE OINT	LACRILUBE S.O.P. EYE OINT
LATANOPROST 0.005% OPHTH DROP	XALATAN 0.005% OPHTH DROP
SODIUM CHLORIDE 5% OPTH DROP	ADSORBONAC 5% OPTH DROP
TIMOLOL 0.5% OPTH DROP	TIMOPTIC 0.5% OPTH DROP

Category: GASTROINTESTINAL DRUGS
Subcategory: Antacids and Adsorbents

MAALOX EXTRA STRENGTH LIQUID	MAALOX EXTRA STRENGTH LIQUID
SODIUM BICARBONATE 650MG TAB	SODIUM BICARBONATE 650MG TAB

Subcategory: Antidiarrhea Agents

DIPHENOXYLATE/ATROPINE TAB	LOMOTIL TAB
LOPERAMIDE 2MG CAP	IMODIUM 2MG CAP
PAREGORIC LIQ	PAREGORIC LIQ

Subcategory: Cathartics and Laxatives

BISACODYL 10MG SUPP	DULCAGEN 10MG SUPP
COLYTE SOLUTION	COLYTE SOLUTION

Subcategory: Digestants

PANCRELIPASE CAP	COTAZYM CAP

Subcategory: Antiemetics

MECLIZINE HCL 12.5MG TAB	BONINE 12.5MG TAB
MECLIZINE HCL 25MG TAB	BONINE 25MG TAB

Generic Name	Trade Name
PROCHLORPERAZINE 25MG SUPP	COMPAZINE 25MG SUPP
PROCHLORPERAZINE 5MG TAB	COMPAZINE 5MG TAB
TRIMETHOBENZAMIDE 100MG SUPP	TIGAN 100MG SUPP
TRIMETHOBENZAMIDE 200MG SUPP	TIGAN 200MG SUPP

Subcategory: Misc GI Drugs

METOCLOPRAMIDE 10MG TAB	METOCLOPRAMIDE 10MG TAB
METOCLOPRAMIDE 5MG/5ML SYRUP	REGLAN 5MG/5ML SYRUP
OMEPRAZOLE 20MG OTC TAB 14’s	PRILOSEC 20MG OTC TAB 14’s
OMEPRAZOLE 20MG OTC TAB 28’s	PRILOSEC 20MG OTC TAB 28’s
RANITIDINE 150MG TAB	ZANTAC 150MG TAB
SUCRALFATE 1GM TAB	CARAFATE 1GM TAB

Category: GOLD COMPOUNDS

AURANOFIN 3MG CAP	RIDAURA 3MG CAP

Category: HEAVY METAL ANTAGONISTS

PENICILLAMINE 250MG CAP	CUPRIMINE 250MG CAP
SUCCIMER 100MG CAP	CHEMET 100MG CAP

Category: HORMONES AND SYNTHETIC SUBSTITUTES
Subcategory: Adrenals

BECLOMETHASONE INHALER	VANCERIL INHALER
BUDESONIDE INH SUSP 0.25MG	PULMICORT RESPULES 0.25 INH SUSP
** Restriction: Patient less than 4 years old **	
BUDESONIDE INH SUSP 0.5MG	PULMICORT RESPULES 0.5 INH SUSP
** Restriction: Patient less than 4 years old **	
DEXAMETHASONE 0.5MG TAB	DECADRON 0.5MG TAB
DEXAMETHASONE 4MG TAB	DECADRON 4MG TAB
FLUDROCORTISONE 0.1MG TAB	FLORINEF 0.1MG TAB
FLUTICASONE PROPIO 110 INHALER	FLOVENT 110MCG INHALER
FLUTICASONE PROPION 44 INHALER	FLOVENT 44MCG INHALER
METHYLPREDNISOLONE 4MG DOSEPAK	MEDROL 4MG DOSEPAK
METHYLPREDNISOLONE 4MG TAB	MEDROL 4MG TAB
PREDNISONE 20MG TAB	DELTASONE 20MG TAB
PREDNISONE 5MG TAB	DELTASONE 5MG TAB
PREDNISONE 5MG/5ML ORAL SOL	PREDNISONE 5MG/5ML ORAL SOL

Subcategory: Contraceptives

LO/OVRAL-28 TAB	LO/OVRAL-28 TAB
NORDETTE-28 TAB	NORDETTE-28 TAB
NORETHINDRONE 0.35MG TAB	MICRONOR 0.35MG TAB
ORTHO EVRA PATCH	ORTHO EVRA PATCH
ORTHO NOVUM-1/35 28 DAYS TAB	ORTHO NOVUM-1/35 28 DAYS TAB

Generic Name	Trade Name
ORTHO NOVUM-777 28 DAYS TAB	ORTHO NOVUM-777 28 DAYS TAB
ORTHO-NOVUM 1/50 TAB	ORTHO-NOVUM 1/50 TAB
TRIPHASIL-28 TAB	TRIPHASIL-28 TAB

Subcategory: Estrogens

ESTROGENS, CONJ 0.625MG TAB	PREMARIN 0.625MG TAB
ESTROGENS, CONJ 1.25MG TAB	PREMARIN 1.25MG TAB
ESTROGENS, CONJ VAG CR W/APP	PREMARIN VAG CR W/APP
CONJ ESTROG/MEDROXYPROG 2.5MG	PREMPRO 2.5MG TAB

Subcategory: Antidiabetic Agents
Subcategory: Insulins

INSULIN GLARGINE 100U/ML VIAL	LANTUS 100U/ML VIAL
INSULIN HUMAN SEMI NPH 100U/ML	NOVOLIN NPH 100U/ML VIAL
INSULIN HUMAN SEMISY L 100U/ML	NOVOLIN LENTE 100U/ML VIAL
INSULIN HUMAN SEMISY R 100U/ML	NOVOLIN REGULAR 100U/ML VIAL
INSULIN HUMAN SEMISYNTH 70/30	NOVOLIN 70/30 100U/ML VIAL

Subcategory: Sulfonylureas

GLIPIZIDE 5MG TAB	GLUCOTROL 5MG TAB
GLYBURIDE 5MG TAB	MICRONASE 5MG TAB

Subcategory: Misc Antidiabetic Agents

METFORMIN HCL 500MG TAB	GLUCOPHAGE 500MG TAB
METFORMIN HCL 850MG TAB	GLUCOPHAGE 850MG TAB
METFORMIN XR 500MG TAB	GLUCOPHAGE XR 500MG TAB
ROSIGLITAZONE 2MG TAB	AVANDIA 2MG TAB
ROSIGLITAZONE 4MG TAB	AVANDIA 4MG TAB
ROSIGLITAZONE 8MG TAB	AVANDIA 8MG TAB

Subcategory: Progestins

MEDROXYPROGESTERONE 10MG TAB	PROVERA 10MG TAB

Subcategory: Thyroid and Antithyroid Agents
Subcategory: Thyroid Agents

LEVOTHYROXINE 0.025MG TAB	LEVOTHROID 0.025MG TAB
LEVOTHYROXINE 0.05MG TAB	SYNTHROID 0.05MG TAB

Generic Name	Trade Name
LEVOTHYROXINE 0.075MG TAB	SYNTHROID 0.075MG TAB
LEVOTHYROXINE 0.125MG TAB	SYNTHROID 0.125MG TAB
LEVOTHYROXINE 0.15MG TAB	SYNTHROID 0.15MG TAB
LEVOTHYROXINE 0.1MG TAB	SYNTHROID 0.1MG TAB
LIOTHYRONINE 25MCG TAB	CYTOMEL 25MCG TAB

Subcategory: Antithyroid Agents

PROPYLTHIOURACIL 50MG TAB	PROPYLTHIOURACIL 50MG TAB

Category: OXYTOCICS

METHYLERGONOVINE 0.2MG TAB	METHERGINE 0.2MG TAB

Category: SKIN AND MUCCOUS MEMBRANE AGENTS
Subcategory: Anti-infectives
Subcategory: Antibiotics

CLINDAMYCIN T 1% SOLUTION	CLEOCIN T 1% SOLUTION
GENTAMICIN 0.1% TOPICAL CREAM	GARAMYCIN 0.1% TOPICAL CREAM
MUPIROCIN 2% OINT	BACTROBAN 2% OINT
NEOMYCI/BACITRACI/POLYMIX OINT	MYCITRACIN OINT

Subcategory: Antivirals

ACYCLOVIR 5% OINT	ZOVIRAX 5% OINT

Subcategory: Antifungals

CLOTRIMAZOLE 10MG TROCHE	MYCELEX 10MG TROCHE
ECONAZOLE 1% TOPICAL CREAM	SPECTAZOLE 1% TOPICAL CREAM
KETOCONAZOLE 2% CREAM	NIZORAL 2% CREAM
NYSTATIN 100000U/GM CREAM	NILSTAT 100000U/GM CREAM
NYSTATIN 100000U/GM OINT	NILSTAT 100000U/GM OINT
TERCONAZOLE VAG 0.4% CREAM	TERAZOL-7 VAG CREAM
TERCONAZOLE VAG 0.8% CREAM	TERAZOL-3 VAG CREAM

Subcategory: Scabicides and Pediculicides

PERMETHRIN 1% CREME RINSE LIQ	NIX 1% CREME RINSE LIQUID
PERMETHRIN 5% CREAM	ELIMITE 5% CREAM
PIPERONYL/PYRETHRIN LIQUID	RID LIQUID

Generic Name	Trade Name

Subcategory: Misc. Local Anti-infectives

SELENIUM 2.5% LOTION SHAMPOO	SELSUN 2.5% LOTION SHAMPOO
SILVER SULFADIAZINE 1% CREAM	SSD 1% CREAM

Subcategory: Anti-inflammatory Agents

DIFLORASONE 0.05% CREAM	MAXIFLOR 0.05% CREAM
DIFLORASONE 0.05% OINT	MAXIFLOR 0.05% OINT
FLUOCINOLONE ACETONI 0.025% CR	SYNEMOL 0.025% CREAM
HYDROCORTISONE 1% CREAM	HYDROCORTISONE 1% CR
HYDROCORTISONE 1% OINT	HYDROCORTISONE 1% OINT
HYDROCORTISONE 100MG ENEMA	CORTENEMA 100MG ENEMA
HYDROCORTISONE 25MG SUPP	ANUSOL HC 25MG SUPP
HYDROCORTISONE ACET 2.5% CREAM	ANUSOL-HC 2.5% CREAM
TRIAMCINOLONE 0.1% PASTE	KENALOG IN ORABASE 0.1% PASTE

Subcategory: Antipruritics and Local Anesthetics

CETACAINE 56GM SPRAY	CETACAINE 56GM SPRAY
LIDOCAINE HCL 5% OINT	XYLOCAINE 5% OINT
PHENAZOPYRIDINE 100MG TAB	PYRIDIUM 100MG TAB

Subcategory: Keratolytic Agents

SALICYLIC ACID 5% IN AQUAPHOR	SALICYLIC ACID 5% IN AQUAPHOR

Subcategory: Keratoplastic Agents

LCD 5% IN AQUAPHOR	LCD 5% IN AQUAPHOR

Subcategory: Misc. Skin and Mucous Membrane Agents

MENTHOL 1/4% IN AQUAPHOR	MENTHOL 1/4% IN AQUAPHOR
PAPAIN-UREA 1.lMU-100MG/GM OIN	ACCUZYME TOPICAL OINT

Category: SMOOTH MUSCLE RELAXANTS
Subcategory: Genitourinary Smooth Muscle Relaxants

OXYBUTYNIN 5MG TAB	DITROPAN 5MG TAB

Generic Name	Trade Name

Subcategory: Respiratory Smooth Muscle Relaxants

AMINOPHYLLINE 200MG TAB	AMINOPHYLLINE 200MG TAB
THEOPHYLLINE 200MG TAB SR	THEODUR 200MG TAB SR
THEOPHYLLINE 300MG TAB SR	THEODUR 300MG TAB SR
THEOPHYLLINE 80MG/15ML ELIX	ELIXOPHYLLIN 80MG/15ML ELIX

Category: VITAMINS
Subcategory: Vitamin B Complex

FOLIC ACID 1MG TAB	FOLIC ACID 1MG TAB
PYRIDOXINE 50MG TAB	VITAMIN B-6 50MG TAB

Subcategory: Vitamin D

CALCITRIOL 0.25MCG CAP	ROCALTROL 0.25MCG CAP

Subcategory: Vitamin K Activity

PHYTONADIONE 5MG TAB	MEPHYTON 5MG TAB

Subcategory: Multivitamin Preparations

STUARTNATAL 1+1 TABLET	STUARTNATAL 1+1 TABLET
VIT B COMPLX/VIT C/PLUS FE TAB	NEPHRO-VITE PLUS IRON TAB

Category: UNCLASSIFIED THERAPEUTIC AGENTS

ALLOPURINOL 100MG TAB	ZYLOPRIM 100MG TAB
ALLOPURINOL 300MG TAB	ZYLOPRIM 300MG TAB
AZATHIOPRINE 50MG TAB	IMURAN 50MG TAB
BROMOCRIPTINE 2.5MG TAB	PARLODEL 2.5MG TAB
CLOPIDOGREL 75MG TAB	PLAVIX 75MG TAB
COLCHICINE 0.6MG TAB	COLCHICINE 0.6MG TAB
CYCLOSPORINE 100MG/ML SOLN	SANDIMMUNE 100MG/ML SOLN
ETIDRONATE 200MG TAB	DIDRONEL 200MG TAB
LEUCOVORIN CALCIUM 25MG TAB	WELLCOVORIN 25MG TAB
LEUCOVORIN CALCIUM 5MG TAB	WELLCOVORIN 5MG TAB
MONTELUKAST 10MG TAB	SINGULAIR 10MG TAB
MONTELUKAST 5MG CHEW TAB	SINGULAIR 5MG CHEW TAB

Category: DEVICES

INSULIN 1ML U-100 SYRINGE	INSULIN 1ML U-100 SYRINGE

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
ACETAMINO 120/COD 12MG/5ML ELIX	TYLENOL W/CODEINE ELIXIR	16
ACETAMINO 300/CODEINE 30MG TAB	TYLENOL w/ CODEINE NO.3 TAB	16
ACETAMINOPHEN 100MG/ML DROP	TYLENOL 100MG/ML DROP	17
ACETAMINOPHEN 160MG/5ML LIQ	TYLENOL 160MG/5ML ELX	17
ACETAZOLAMIDE 250MG TAB	DIAMOX 250MG TAB	22
ACETAZOLAMIDE 500MG CAP	DIAMOX SEQUELS 500MG CAP	22
ACETIC ACID 2% OTIC SOL	VOSOL 2% OTIC SOL	22
ACETIC ACID 2%/HC 1% OTIC SOL	VOSOL HC OTIC SOL	22
ACYCLOVIR 200MG CAP	ZOVIRAX 200MG CAP	11
ACYCLOVIR 5% OINT	ZOVIRAX 5% OINT	26
ALBUTEROL 2MG TAB	PROVENTIL 2MG TAB	13
ALBUTEROL 2MG/5ML SYRUP	PROVENTIL 2MG/5ML SYRUP	13
ALBUTEROL 4MG REPETAB	PROVENTIL 4MG REPETAB	13
ALBUTEROL 4MG TAB	PROVENTIL 4MG TAB	13
ALBUTEROL METERED INHALER	PROVENTIL METERED INHALER	13
ALBUTEROL 0.083% NEB UD SOL	PROVENTIL 0.083% NEB UD SOL	13
ALBUTEROL/IPRATROPIUM INH	COMBIVENT INHALER	13
ALLOPURINOL 100MG TAB	ZYLOPRIM 100MG TAB	28
ALLOPURINOL 300MG TAB	ZYLOPRIM 300MG TAB	28
ALPRAZOLAM 0.25MG TAB	XANAX 0.25MG TAB	18
ALPRAZOLAM 0.5MG TAB	XANAX 0.5MG TAB	18
ALPRAZOLAM 1MG TAB	XANAX 1MG TAB	18
AMINOPHYLLINE 200MG TAB	AMINOPHYLLINE 200MG TAB	28
AMIODARONE 200MG TAB	CORDARONE 200MG TAB	14
AMITRIPTYLINE 10MG TAB	ELAVIL 10MG TAB	18
AMITRIPTYLINE 25MG TAB	ELAVIL 25MG TAB	18
AMITRIPTYLINE HCL 50MG TAB	ELAVIL 50MG TAB	18
AMLODIPINE BESYLATE 10MG TAB	NORVASC 10MG TAB	14
AMLODIPINE BESYLATE 5MG TAB	NORVASC 5MG TAB	14
AMOXICILLIN 125/CLAV 31.2 SUSP	AUGMENTIN 125 SUSP	10
AMOXICILLIN 125MG/5ML SUSP	TRIMOX 125/5ML SUSP	10
AMOXICILLIN 250/CLAV 125 TAB	AUGMENTIN 250MG TAB	11
AMOXICILLIN 250/CLAV 62.5MG SUSP	AUGMENTIN 250 SUSP	11
AMOXICILLIN 250MG CAP	AMOXICILLIN 250MG CAP	11
AMOXICILLIN 250MG/5ML SUSP	TRIMOX 250MG/5ML SUSP	11
AMOXICILLIN 500/CLAV 125 TAB	AUGMENTIN 500MG TAB	11
AMOXICILLIN 500MG CAP	AMOXICILLIN 500MG CAP	11
AMOXICILLIN 875/CLAV 125 TAB	AUGMENTIN 875MG TAB	11
ATENOLOL 50MG TAB	TENORMIN 50MG TAB	14
ATORVASTATIN 80MG TAB	LIPITOR 80MG TAB	15
** PRIOR AUTHORIZATION REQUIRED **		
ATROPINE 1% OPTH DROP	ATROPINE 1% OPTH DROP	22
AURALGAN EAR DROP	AURALGAN EAR DROP	22
AURANOFIN 3MG CAP	RIDAURA 3MG CAP	23
AZATHIOPRINE 50MG TAB	IMURAN 50MG TAB	28
AZITHROMYCIN 250MG CAP (Z-PAK)	ZITHROMAX 250MG CAP (Z-PAK	10
AZITHROMYCIN 600MG/15ML SUSP	ZITHROMAX 600MG/15ML ORAL	10
AZITHROMYCIN 900MG/22.5ML SUSP	ZITHROMAX 900MG/22.5ML SUSP	10

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
BACITRACIN 500U/GM EYE OINT	BACITRACIN 500U/GM EYE OINT	21
BACLOFEN 10MG TAB	LIORESAL 10MG TAB	14
BECLOMETHASONE INHALER	VANCERIL INHALER	23
BENZTROPINE 1MG TAB	COGENTIN 1MG TAB	13
BENZTROPINE 2MG TAB	COGENTIN 2MG TAB	13
BETAXOLOL HCL 0.25% OPTH	BETOPTIC S 0.25% OPTH DROP	23
BETHANECHOL 25MG TAB	URECHOLINE 25MG TAB	13
BETHANECHOL 5MG TAB	URECHOLINE 5MG TAB	13
BETHANECOL 10MG TAB	URECHOLINE 10MG TAB	13
BICITRA SUGAR FREE SOL	BICITRA SUGAR FREE SOLUTION	20
BISACODYL 10MG SUPP	DULCAGEN 10MG SUPP	23
BRIMONIDINE 0.2% OPHTH DROP	ALPHAGAN 0.2% OPHTH DROP	23
BROMOCRIPTINE 2.5MG TAB	PARLODEL 2.5MG TAB	28
BUDESONIDE INH SUSP 0.25MG	PULMCORT RESPULS 0.25MG INH SUSP	24
** Restriction: Patient less than 4 years old **		
BUDESONIDE INH SUSP 0.5MG	PULMCORT RESPULS 0.5MG INH SUSP	24
** Restriction: patient less than 4 years old **		
BUMETANIDE 1MG TAB	BUMEX 1MG TAB	20
BUSULFAN 2MG TAB	MYLERAN 2MG TAB	12
BUTALB 50/CAFF 40/ASA 325 TAB	FIORINAL TAB	16
CALCITRIOL 0.25MCG CAP	ROCALTROL 0.25MCG CAP	28
CALCIUM CARBONATE 650MG TAB	CALCIUM CARBONATE 650MG TAB	20
CAPTOPRIL 12.5MG TAB	CAPOTEN 12.5MG TAB	14
CAPTOPRIL 25MG TAB	CAPOTEN 25MG TAB	14
CARBAMAZEPINE 100MG TAB	TEGRETOL 100MG TAB	17
CARBAMAZEPINE 100MG/5ML SUSP	TEGRETOL 100MG/5ML SUSP	17
CARBAMAZEPINE 200MG TAB	TEGRETOL 200MG TAB	17
CARBIDOPA/LEVADOPA 10/100 TAB	SINEMET-10/100 TABLET	19
CARBIDOPA/LEVADOPA 25/100 TAB	SINEMET-25/100 TABLET	19
CARBIDOPA/LEVADOPA 25/250 TAB	SINEMET-25/250 TABLET	19
CEPHALEXIN 125MG/5ML ORAL	KEFLEX 125MG/5ML ORAL SUSP	10
CEPHALEXIN 250MG CAP	KEFLEX 250MG CAP	10
CEPHALEXIN 500MG CAP	KEFLEX 500MG CAP	10
CERUMENEX 10% EAR DROP	CERUMENEX 10% EAR DROP	23
CETACAINE 56GM SPRAY	CETACAINE 56GM SPRAY	27
CHLORAMBUCIL 2MG TAB	LEUKERAN 2MG TAB	12
CHLORDIAZEPOXIDE 10MG CAP	LIBRIUM 10MG CAP	18
CHLORDIAZEPOXIDE 25MG CAP	LIBRIUM 25MG CAP	18
CHLORDIAZEPOXIDE 5MG CAP	LIBRIUM 5MG CAP	18
CHLORPROMAZINE 25MG TAB	THORAZINE 25MG TAB	18
CHLORPROMAZINE 50MG TAB	THORAZINE 50MG TAB	18
CHOLESTYRAMINE LIGHT PKT	QUESTRAN LIGHT PKT	15
CIPROFLOXACIN 0.3% EYE OINT	CILOXAN 0.3% EYE OINT	21
CIPROFLOXACIN 0.3% OPTH DROP	CILOXAN 0.3% OPTH DROP	21
CIPROFLOXACIN HCL 250MG TAB	CIPRO 250MG TAB	12
CIPROFLOXACIN HCL 500MG TAB	CIPRO 500MG TAB	12
CIPROFLOXACIN HCL 750MG TAB	CIPRO 750MG TAB	12
CLARITHROMYCIN 250MG TAB	BIAXIN 250MG TAB	10
CLARITHROMYCIN 500MG TAB	BIAXIN 500MG TAB	10
CLINDAMYCIN 150MG CAP	CLEOCIN 150MG CAP	11
CLINDAMYCIN T 1% SOLUTION	CLEOCIN T 1% SOLUTION	26

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
CLONAZEPAM 0.5MG TAB	KLONOPIN 0.5MG TAB	17
CLONAZEPAM 1MG TAB	KLONOPIN 1MG TAB	17
CLONAZEPAM 2MG TAB	KLONOPIN 2MG TAB	17
CLONIDINE HCL 0.1MG TAB	CATAPRES 0.1MG TAB	15
CLONIDINE HCL 0.2MG TAB	CATAPRES 0.2MG TAB	15
CLONIDINE HCL 0.3MG TAB	CATAPRES 0.3MG TAB	15
CLONIDINE-TTS 1 PATCH	CATAPRES-TTS 1 PATCH	15
CLONIDINE-TTS 2 PATCH	CATAPRES-TTS 2 PATCH	15
CLONIDINE-TTS 3 PATCH	CATAPRES-TTS 3 PATCH	15
CLOPIDOGREL 75MG TAB	PLAVIX 75MG TAB	28
CLOTRIMAZOLE 10MG TROCHE	MYCELEX 10MG TROCHE	26
CODEINE SULFATE 30MG TAB	CODEINE 30MG TAB	16
COLCHICINE 0.6MG TAB	COLCHICINE 0.6MG TAB	28
COLY-MYCIN S OTIC DROP	COLY-MYCIN S OTIC DROP	21
COLYTE SOLUTION 4000ML	COLYTE SOLUTION 4000ML	23
CONDOMS LUBRICATED/SPERMICIDAL	CONDOMS LUBRICATED/SPERM	19
CONJ ESTROG/MEDROXYPROG 2.5MG TAB	PREMPRO 2.5MG TAB	25
CYCLOBENZAPRINE 10MG TAB	FLEXERIL 10MG TAB	14
CYCLOPENTOL/PHENYLEPH OPTH SOL	CYCLOMYDRIL OPTH SOL	22
CYCLOPENTOLATE 1% OPTH DROP	CYCLOGYL 1% OPTH DROP	22
CYCLOSPORINE 100MG/ML SOL	SANDIMMUNE 100MG/ML SOL	28
DAPSONE 100MG TAB	DAPSONE 100MG TAB	12
DAPSONE 25MG TAB	DAPSONE 25MG TAB	12
DELFEN FOAM 12.5% VAGINAL	DELFEN FOAM 12.5% VAGINAL	19
DESIPRAMINE 10MG TAB	NORPRAMIN 10MG TAB	18
DESIPRAMINE 25MG TAB	NORPRAMINE 25MG TAB	18
DESIPRAMINE 50MG TAB	NORPRAMIN 50MG TAB	18
DEXAMETHASONE 0.5MG TAB	DECADRON 0.5MG TAB	24
DEXAMETHASONE 4MG TAB	DECADRON 4MG TAB	24
DIAPHRAGM ARC-SPRING 65MM	ORTHO-DIAPHRAGM ALLFLX 65	19
DIAPHRAGM ARC-SPRING 70MM	ORTHO-DIAPHRAGM ALLFLX 70	19
DIAPHRAGM ARC-SPRING 75MM	ORTHO-DIAPHRAGM ALLFLX 75	19
DIAPHRAGM ARC-SPRING 80MM	ORTHO-DIAPHRAGM ALLFLX 80	19
DIAPHRAGM ARC-SPRING 85MM	ORTHO-DIAPHRAGM ALLFLX 85	19
DIAZEPAM 5MG TAB	VALIUM 5MG TAB	19
DICLOXACILLIN 250MG CAP	PATHOCIL 250MG CAP	11
DICYCLOMINE 10MG CAP	BENTYL 10MG CAP	13
DIFLORASONE 0.05% CREAM	MAXIFLOR 0.05% CREAM	27
DIFLORASONE 0.05% OINT	MAXIFLOR 0.05% OINT	27
DIGOXIN 0.05MG/ML ELIXIR	LANOXIN 0.05MG/ML ELIXIR	14
DIGOXIN 0.125MG TAB	LANOXIN 0.125MG TAB	14
DIGOXIN 0.25MG TAB	LANOXIN 0.25MG TAB	14
DILTIAZEM 180MG CR CAP	TIAZAC 180MG CR CAP	14
DILTIAZEM 30MG TAB	CARDIZEM 30MG TAB	14
DILTIAZEM 60MG TAB	CARDIZEM 60MG TAB	14
DILTIAZEM HCL 240MG CR CAP	TIAZAC 240MG CR CAP	14
DILTIAZEM HCL 300MG CR CAP	TIAZAC 300MG CR CAP	14
DIPHENHYDRAMINE 12.5MG/5ML ELIXIR	BENADRYL 12.5MG/5ML ELIXIR	10
DIPHENHYDRAMINE 25MG CAP	BENADRYL 25MG CAP	10
DIPHENOXYLATE/ATROPINE TAB	LOMOTIL TAB	23
DIPIVEFRIN 0.1% OPTH DROP	PROPINE 0.1% OPTH DROP	22

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
DIPYRIDAMOLE 25MG TAB	PERSANTINE 25MG TAB	16
DORZOLAMIDE HCL 2% OPTH DROP	TRUSOPT 2% OPTH DROP	22
DOXAZOSIN MESYLATE 1MG TAB	CARDURA 1MG TAB	15
DOXAZOSIN MESYLATE 2MG TAB	CARDURA 2MG TAB	15
DOXAZOSIN MESYLATE 4MG TAB	CARDURA 4MG TAB	15
DOXYCYCLINE 100MG CAP	VIBRAMYCIN 100MG CAP	11
ECONAZOLE 1% TOPICAL CREAM	SPECTAZOLE 1% TOPICAL CREAM	26
ERGOTAMINE 1MG/CAFF 100MG	CAFERGOT TABLET	14
ERYTHROMYCIN 200MG/5ML SUSP	E.E.S. 200MG/5ML SUSP	10
ERYTHROMYCIN 250MG FILMTAB	E.E.S 250MG FILMTAB	10
ERYTHROMYCIN EYE OINT	ILOTYCIN EYE OINT	21
ERYTHROMYCIN/SULFISOX ORAL SUSP	PEDIAZOLE ORAL SUSP	12
ESTROGENS, CONJ 0.625MG TAB	PREMARIN 0.625MG TAB	25
ESTROGENS, CONJ 1.25MG TAB	PREMARIN 1.25MG TAB	25
ESTROGENS, CONJ VAG CR W/APP	PREMARIN VAG CR W/APP	25
ETHAMBUTOL 100MG TAB	MYAMBUTOL 100MG TAB	11
ETHAMBUTOL 400MG TAB	MYAMBUTOL 400MG TAB	11
ETIDRONATE 200MG TAB	DIDRONEL 200MG TAB	28
FERROUS SULF 325MG TAB UD	FERROUS SULF 325MG TAB UD	14
FERROUS SULF 220MG/5ML ELIXIR	FERROUS SULF 220MG/5ML ELIX	14
FLUCONAZOLE 150MG TAB	DIFLUCAN 150MG TAB	10
FLUDROCORTISONE 0.1MG TAB	FLORINEF 0.1MG TAB	24
FLUNISOLIDE 0.025% NASAL INH	NASALIDE 0.025% NASAL INH	22
FLUOCINOLONE ACETONI 0.025% CREAM	SYNEMOL 0.025% CREAM	27
FLUOROMETHOLONE EYE OINT	FML EYE OINT	22
FLUPHENAZINE 5MG TAB	PROLIXIN 5MG TAB	18
FLUPHENAZINE HCL 1MG TAB	PROLIXIN 1MG TAB	18
FLURAZEPAM 15MG CAP	DALMANE 15MG CAP	19
FLUTICASONE PROPIO 110MCG INHALER	FLOVENT 110MCG INHALER	24
FLUTICASONE PROPION 44MCG INHALER	FLOVENT 44MCG INHALER	24
FOLIC ACID 1MG TAB	FOLIC ACID 1MG TAB	28
FOSINOPRIL SODIUM 10MG TAB	MONOPRIL 10MG TAB	14
FOSINOPRIL SODIUM 20MG TAB	MONOPRIL 20MG TAB	14
FOSINOPRIL SODIUM 40MG TAB	MONOPRIL 40MG TAB	15
FUROSEMIDE 20MG TAB	LASIX 20MG TAB	20
FUROSEMIDE 40MG TAB	LASIX 40MG TAB	20
GABAPENTIN 300MG CAP	NEURONTIN 300MG CAP	17
GABAPENTIN 400MG CAP	NEURONTIN 400MG CAP	17
GASTROGRAFFIN SOLUTION	GASTROGRAFFIN SOLUTION	19
GENTAMICIN 0.1% TOPICAL CREAM	GARAMYCIN 0.1% TOPICAL CR	26
GENTAMICIN 3MG/ML OPTH DROP	GARAMYCIN 3MG/ML OPTH DROP	21
GENTAMICIN SULF EYE OINT	GARAMYCIN EYE OINT	21
GLIPIZIDE 5MG TAB	GLUCOTROL 5MG TAB	25
GLYBURIDE 5MG TAB	MICRONASE 5MG TAB	25
GRANULEX SPRAY	GRANULEX SPRAY	21
GRISEOFULVIN 125MG/5ML SUSP	GRIFULVIN V 125MG/5ML SUSP	10
GRISEOFULVIN 250MG TAB	GRIFULVIN V 250MG TAB	10
GUAIFENSIN/CODEINE SYRUP	ROBITUSSIN AC SYRUP	21
HALOPERIDOL 1MG TAB	HALDOL 1MG TAB	18
HALOPERIDOL 5MG TAB	HALDOL 5MG TAB	18
HOMATROPINE 2% OPTH DROP	ISOPTO HOMATROPIN 2% OPTH	22
HOMATROPINE 5% OPTH DROP	ISOPTO HOMATROPIN 5% OPTH	22

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
HOMATROPINE 5% OPTH DROP	ISOPTO HOMATROPIN 5% OPTH	22
HYDRALAZINE 25MG TAB	APRESOLINE 25MG TAB	15
HYDRALAZINE 50MG TAB	APRESOLINE 50MG TAB	15
HYDROCHLOROTHIAZIDE 25MG TAB	ESIDREX 25MG TAB	20
HYDROCHLOROTHIAZIDE 50MG TAB	ESIDREX 50MG TAB	20
HYDROCORTISONE 1% CREAM	HYDROCORTISONE 1% CREAM	27
HYDROCORTISONE 1% OINT	HYDROCORTISONE 1% OINT	27
HYDROCORTISONE 100MG ENEMA	CORTENEMA 100MG ENEMA	27
HYDROCORTISONE 25MG SUPP	ANUSOL HC 25MG SUPP	27
HYDROCORTISONE ACET 2.5% CREAM	ANUSOL-HC 2.5% CREAM	27
HYDROMORPHONE 2MG TAB	DILAUDID 2MG TAB	16
HYDROXYCHLOROQUINE 200MG TAB	PLAQUENIL 200MG TAB	11
HYDROXYPROPYLMETH 2.5% OPTH SOL	GONIOSOL 2.5% OPTH SOL	23
HYDROXYUREA 500MG CAP	HYDREA 500MG CAP	12
HYDROXYZINE 10MG/5ML SYRUP	ATARAX 10MG/5ML SYRUP	19
HYDROXYZINE HCL 10MG TAB	ATARAX 10MG TAB	19
HYDROXYZINE HCL 25MG TAB	ATARAX 25MG TAB	19
HYPOTEARS OPTH DROP	HYPOTEARS OPTH DROP	23
IBUPROFEN 400MG TAB	MOTRIN 400MG TAB	16
IBUPROFEN 600MG TAB	MOTRIN 600MG TAB	16
IMIPRAMINE 25MG TAB	TOFRANIL 25MG TAB	18
IMIPRAMINE HCL 10MG TAB	TOFRANIL 10MG TAB	18
INDOMETHACIN 25MG CAP	INDOCIN 25MG CAP	16
INSULIN 1ML U-100 SYRINGE	INSULIN 1ML U-100 SYRINGE	28
INSULIN GLARGINE 100U/ML VIAL	LANTUS 100U/ML VIAL	25
INSULIN HUMAN SEMI NPH 100U/ML VIAL	NOVOLIN NPH 100U/ML VIAL	25
INSULIN HUMAN SEMISY L 100U/ML VIAL	NOVOLIN LENTE 100U/ML VIAL	25
INSULIN HUMAN SEMISY R 100U/ML VIAL	NOVOLIN REGULAR 100U/ML VIAL	25
INSULIN HUMAN SEMISYNTH 70/30 VIAL	NOVOLIN 70/30 100U/ML VIAL	25
IPRATROPIUM BR INHALER	ATROVENT INHALER	13
ISONIAZID 100MG TAB	ISONIAZID 100MG TAB	11
ISONIAZID 300MG TAB	ISONIAZID 300MG TAB	11
ISONIAZID 50MG/5ML SYRUP	ISONIAZID 50MG/5ML SYRUP	11
ISOSORBIDE MONONIT 120MG TAB	IMDUR 120MG TAB CREAM	16
ISOSORBIDE MONONIT 30MG TAB CREAM	IMDUR 30MG TAB CREAM	16
ISOSORBIDE MONONIT 60MG TAB CREAM	IMDUR 60MG TAB CREAM	16
KETOCONAZOLE 2% CREAM	NIZORAL 2% CREAM	26
KETOPROFEN 50MG CAP	ORUDIS 50MG CAP	16
KETOROLAC TROM 0.5% OPTH DROP	ACULAR 0.5% OPTH DROP	22
LABETALOL 100MG TAB	NORMODYNE 100MG TAB	15
LABETALOL 200MG TAB	NORMODYNE 200MG TAB	16
LACRILUBE EYE OINT	LACRILUBE S.O.P. EYE OINT	23
LACTULOSE 10GM/15ML SYRUP	CEPHULAC 10GM/15ML SYRUP	20
LAMOTRIGINE 100MG TAB	LAMICTAL 100MG TAB	17
LAMOTRIGINE 25MG TAB	LAMICTAL 25MG TAB	17
LATANOPROST 0.005% OPHTH DROP	XALATAN 0.005% OPHTH DROP	23
LCD 5% IN AQUAPHOR	LCD 5% IN AQUAPHOR	27
LEUCOVORIN CALCIUM 25MG TAB	WELLCOVORIN 25MG TAB	28
LEUCOVORIN CALCIUM 5MG TAB	WELLCOVORIN 5MG TAB	28
LEVOFLOXACIN 250MG TAB	LEVAQUIN 250MG TAB	12

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
LEVOFLOXACIN 500MG TAB	LEVAQUIN 500MG TAB	12
LEVOFLOXACIN 750MG TAB	LEVAQUIN 750MG TAB	12
LEVOTHYROXINE 0.025MG TAB	LEVOTHROID 0.025MG TAB	25
LEVOTHYROXINE 0.05MG TAB	SYNTHROID 0.05MG TAB	25
LEVOTHYROXINE 0.075MG TAB	SYNTHROID 0.075MG TAB	26
LEVOTHYROXINE 0.125MG TAB	SYNTHROID 0.125MG TAB	26
LEVOTHYROXINE 0.15MG TAB	SYNTHROID 0.15MG TAB	26
LEVOTHYROXINE 0.1MG TAB	SYNTHROID 0.1MG TAB	26
LIDOCAINE 2% VISCOUS SOL	LIDOCAINE 2% VISCOUS SOL	22
LIDOCAINE HCL 2% JELLY	XYLOCAINE 2% JELLY	22
LIDOCAINE HCL 5% OINT	XYLOCAINE 5% OINT	27
LIOTHYRONINE 25MCG TAB	CYTOMEL 25MCG TAB	26
LISINOPRIL 10MG TAB	ZESTRIL 10MG TAB	15
LISINOPRIL 20MG TAB	ZESTRIL 20MG TAB	15
LISINOPRIL 5MG TAB	ZESTRIL 5MG TAB	15
LITHIUM CARBONATE 300MG CAP	ESKALITH 300MG CAP	19
LO/OVRAL-28 TAB	LO/OVRAL-28 TAB	24
LOPERAMIDE 2MG CAP	IMODIUM 2MG CAP	23
LORATADINE 10MG TAB	CLARITIN 10MG TAB	10
LORATADINE 5MG/5ML SYRUP	CLARITIN 5MG/5ML SYRUP	10
LORAZEPAM 0.5MG TAB	ATIVAN 0.5MG TAB	19
LORAZEPAM 1MG TAB	ATIVAN 1MG TAB	19
LORAZEPAM 2MG TAB	ATIVAN 2MG TAB	19
LUGOLS SOLUTION	LUGOLS SOLUTION	21
MAALOX EXTRA STRENGTH LIQ	MAALOX EXTRA STRENGTH LIQ	23
MAGIC MOUTHWASH SOL	MAGIC MOUTHWASH SOL	22
MAXITROL OPTHALMIC DROP	MAXITROL OPTHALMIC DROP	21
MEBENDAZOLE 100MG CHEWABLE TAB	VERMOX 100MG CHEWABLE TAB	10
MECLIZINE HCL 12.5MG TAB	BONINE 12.5MG TAB	23
MECLIZINE HCL 25MG TAB	BONINE 25MG TAB	23
MEDROXYPROGESTERONE 10MG TAB	PROVERA 10MG TAB	25
MEGESTROL 40MG TAB	MEGACE 40MG TAB	12
MEGESTROL 40MG/ML ORAL SUSP	MEGACE 40MG/ML ORAL SUSP	12
MELPHALAN 2MG TAB	ALKERAN 2MG TAB	12
MENTHOL 1/4% IN AQUAPHOR	MENTHOL 1/4% IN AQUAPHOR	27
MEPERIDINE 50MG TAB	DEMEROL 50MG TAB	16
METAPROTERENOL 10MG TAB	ALUPENT 10MG TAB	13
METAPROTERENOL 5% INH SOLUTION	ALUPENT 5% INH SOLUTION	13
METAPROTERENOL METERED INHALER	ALUPENT METERED INHALER	13
METFORMIN XR 500MG TAB	GLUCOPHAGE XR 500MG TAB	25
METFORMIN HCL 500MG TAB	GLUCOPHAGE 500MG TAB	25
METFORMIN HCL 850MG TAB	GLUCOPHAGE 850MG TAB	25
METHAZOLAMIDE 50MG TAB	NEPTAZANE 50MG TAB	22
METHOTREXATE 2.5MG TAB	METHOTREXATE 2.5MG TAB	12
METHYLDOPA 250MG TAB	ALDOMET 250MG TAB	16
METHYLERGONOVINE 0.2MG TAB	METHERGINE 0.2MG TAB	26
METHYLPHENIDATE 10MG TAB	RITALIN 10MG TAB	18
METHYLPREDNISOLONE 4MG DOSEPACK	MEDROL 4MG DOSEPAK	24
METHYLPREDNISOLONE 4MG TAB	MEDROL 4MG TAB	24
METOCLOPRAMIDE 10MG TAB	REGLAN 10MG TAB	24
METOCLOPRAMIDE 5MG/5ML SYRUP	REGLAN 5MG/5ML SYRUP	24

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
METOLAZONE 5MG TAB	DIULO 5MG TAB	20
METOPROLOL 50MG TAB	LOPRESSOR 50MG TAB	15
METRONIDAZOLE 250MG TAB	FLAGYL 250MG TAB	12
MINOXIDIL 10MG TAB	LONITEN 10MG TAB	16
MINOXIDIL 2.5MG TAB	LONITEN 2.5MG TAB	16
MONTELUKAST 10MG TAB	SINGULAIR 10MG TAB	28
MONTELUKAST 5MG CHEW TAB	SINGULAIR 5MG CHEW TAB	28
MORPHINE SUL 20MG/ML-120ML SOL	ROXANOL 20MG/ML-120ML SOL	17
MORPHINE SULFATE 20MG/ML SOL	ROXANOL 20MG/ML SOLN	17
MORPHINE SULFATE 30MG SA TAB	MS CONTIN 30MG SA TAB	17
MUPIROCIN 2% OINT	BACTROBAN 2% OINT	26
NAPROXEN 250MG TAB	NAPROSYN 250MG TAB	16
NAPROXEN 375MG TAB	NAPROSYN 375MG TAB	16
NEOMYC/POLYM B/HC OTIC SUSP	CORTISPORIN OTIC SUSP	21
NEOMYCI/BACITRACI/POLYMIX OINT	MYCITRACIN OINT	26
NIFEDIPINE 10MG CAP	PROCARDIA 10MG CAP	15
NIFEDIPINE CC 30MG TAB	ADALAT CC 30MG TAB	15
NIFEDIPINE CC 60MG TAB	ADALAT CC 60MG TAB	15
NIFEDIPINE CC 90MG TAB	ADALAT CC 90MG TAB	15
NITROFURANTOIN 100MG CAP	MACRODANTIN 100MG CAP	12
NITROFURANTOIN 50MG CAP	MACRODANTIN 50MG CAP	12
NITROGLYCERIN 0.2MG/HR PATCH	TRANSDERM-NITRO 0.2MG/HR	16
NITROGLYCERIN 0.4MG TAB SL	NITROSTAT 0.4MG TAB SL	16
NITROGLYCERIN 0.4MG/HR PATCH	NITRO-DUR 0.4MG/HR PATCH	16
NITROGLYCERIN 0.6MG TAB SL	NITROSTAT 0.6MG TAB SL	16
NITROGLYCERIN 2% OINT	NITROL 2% OINT	16
NORDETTE-28 TAB	NORDETTE-28 TAB	24
NORETHINDRONE 0.35MG TAB	MICRONOR 0.35MG TAB	24
NORTRIPTYLINE HCL 10MG CAP	PAMELOR 10MG CAP	18
NORTRIPTYLINE HCL 25MG CAP	PAMELOR 25MG CAP	18
NYSTATIN 100000U/GM CREAM	NILSTAT 100000U/GM CREAM	26
NYSTATIN 100000U/GM OINT	NILSTAT 100000U/GM OINT	26
NYSTATIN 100000U/ML SUSP	NILSTAT 100000U/ML SUSP	10
OFLOXACIN OTIC 0.3% DROP	FLOXIN OTIC 0.3% DROP	21
OMEPRAZOLE OTC 20MG TAB 14’s	PRILOSEC OTC 20MG TAB 14’s	24
OMEPRAZOLE OTC 20MG TAB 28’s	PRILOSEC OTC 20MG TAB 28’s	24
ORTHO EVRA PATCH	ORTHO EVRA PATCH	24
ORTHO NOVUM-1/35 28 DAY	ORTHO NOVUM-1/35 28 DAY	24
ORTHO NOVUM-777 28 DAY TAB	ORTHO NOVUM-777 28 DAY TAB	25
ORTHO-NOVUM 1/50 28 DAY	ORTHO-NOVUM 1/50 28 DAY	25
OXYBUTYNIN 5MG TAB	DITROPAN 5MG TAB	27
OXYCODONE 5/ACETAMIN 325MG TAB	PERCOCET 5/325MG TAB	17
PANCRELIPASE CAP	COTAZYM CAP	23
PAPAIN-UREA 1.1MU-100MG/GM OINT	ACCUZYME TROPICAL OINT	27
PAREGORIC LIQ	PAREGORIC LIQ	23
PENICILLAMINE 250MG CAP	CUPRIMINE 250MG CAP	24
PENICILLIN VK 250MG TAB	PENICILLIN VK 250MG TAB	11
PENICILLIN VK 250MG/5ML SUSP	LEDERCILLIN VK 250MG/5ML	11
PENTOXIFYLLINE 400MG TAB SA	TRENTAL 400MG TAB SA	14
PERMETHRIN 1% CREME RINSE	NIX 1% CREME RINSE LIQUID	26

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
PERMETHRIN 5% CREAM	ELIMITE 5% CREAM	26
PHENAZOPYRIDINE 100MG TAB	PYRIDIUM 100MG TAB	27
PHENOBARBITAL 20MG/5ML ELIXIR	PHENOBARBITAL 20MG/5ML ELIXIR	18
HENOBARBITAL 30MG TAB	PHENOBARBITAL 30MG TAB	18
PHENYLEPHRINE 2.5% OPTH DROP	NEOSYNEPHRINE 2.5% OPTH DROP	23
PHENYTOIN 100MG CAP	DILANTIN 100MG CAP	17
PHENYTOIN 125MG/5ML SUSP	DILANTIN 125MG/5ML SUSP	17
PHENYTOIN 50MG TAB	DILANTIN 50MG TAB	17
PHENYTOIN SOD 30MG SR CAP	DILANTIN 30MG SR CAP	17
PHYTONADIONE 5MG TAB	MEPHYTON 5MG TAB	28
PILOCARPINE 2% OPTH DROP	PILOCAR 2% OPTH DROP	22
PILOCARPINE 4% EYE GEL	PILOPINE HS 4% EYE GEL	22
PILOCARPINE 4% OPTH DROP	PILOCAR 4% OPTH DROP	22
PIROXICAM 10MG CAP	FELDENE 10MG CAP	16
PIROXICAM 20MG CAP	FELDENE 20MG CAP	16
POTASSIUM CHLORIDE 10% SOL	POTASSIUM CHLORIDE 10% SOL	20
POTASSIUM CHLORIDE 20MEQ PKT	KLOR 20MEQ PKT	20
POTASSIUM CHLORIDE 20MEQ TAB	KLORVESS 20MEQ TAB	20
POTASSIUM CL 10MEQ SA TAB	TEN-K 10MEQ SA TAB	20
PREDNISOLONE ACET 1% OPTH DROP	PRED FORTE 1% OPTH DROP	22
PREDNISONE 20MG TAB	DELTASONE 20MG TAB	24
PREDNISONE 5MG TAB	DELTASONE 5MG TAB	24
PREDNISONE 5MG/5ML ORAL SOL	PREDNISONE 5MG/5ML ORAL SOL	24
PRIMAQUINE 26.3MG TAB	PRIMAQUINE 26.3MG TAB	11
PRIMIDONE 250MG TAB	MYSOLINE 250MG TAB	17
PROBENECID 500MG TAB	BENEMID 500MG TAB	21
PROCAINAMIDE 250MG CAP	PROCAN 250MG CAP	15
PROCAINAMIDE SR 500MG TAB	PROCAN SR 500MG TAB	15
PROCHLORPERAZINE 25MG SUP	COMPAZINE 25MG SUPP	24
PROCHLORPERAZINE 5MG TAB	COMPAZINE 5MG TAB	24
PROMETHAZINE HCL 25MG SUPP	PHENERGAN 25MG SUPP	10
PROMETHAZINE HCL 50MG SUPP	PHENERGAN 50MG SUPP	10
PROPANTHELINE 15MG TAB	PROBANTHINE 15MG TAB	13
PROPARACAINE 0.5% OPTH DROP	OPHTHETIC 0.5% OPTH DROP	22
PROPRANOLOL 10MG TAB	INDERAL 10MG TAB	15
PROPRANOLOL 40MG TAB	INDERAL 40MG TAB	15
PROPRANOLOL LA 120MG CAP	INDERAL LA 120MG CAP	15
PROPRANOLOL LA 160MG CAP	INDERAL LA 160MG CAP	15
PROPRANOLOL LA 80MG CAP	INDERAL LA 80 MG CAP	15
PSEUDOEPHED/CARBINOX DM DROP	RONDEC DM DROP	21
PROPYLTHIOURACIL 50MG TAB	PROPYLTHIOURACIL 50MG TAB	26
PYRAZINAMIDE 500MG TAB	PYRAZINAMIDE 500MG TAB	11
PSEUDOEPHED/CARBINOX DM SYRUP	RONDEC DM SYRUP	21
PYRIDOSTIGMINE 60MG TAB	MESTINON 60MG TAB	13
PYRIDOXINE 50MG TAB	VITAMIN B-6 50MG TAB	28
PYRIMETHAMINE 25MG TAB	DARAPRIM 25MG TAB	11
QUINIDINE GLUCONATE 324MG	QUINAGLUTE 324MG TAB	15
QUINIDINE SULFATE 200MG TAB	QUINORA 200MG TAB	15
RANITIDINE 150MG TAB	ZANTAC 150MG TAB	24
PIPERONYL/PYRETHRIN LIQUID	RID LIQUID	26

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
RIFAMPIN 300MG CAP	RIMACTANE 300MG CAP	11
ROSIGLITAZONE 2MG TAB	AVANDIA 2MG TAB	25
ROSIGLITAZONE 4MG TAB	AVANDIA 4MG TAB	25
ROSIGLITAZONE 8MG TAB	AVANDIA 8MG TAB	25
SALICYLIC ACID 5% IN AQUAPHOR	SALICYLIC ACID 5% IN AQUAPH	27
SALMETEROL XINAFOATE DISKUS 50MCG INH	SEREVENT DISKUS 50MCG INH	13
SALMETROL-FLUTICASON 100/50 DISK INH	ADVAIR 100/50 DISK INH	13
SALMETROL-FLUTICASON 250/50 DISK INH	ADVAIR 250/50 DISK INH	13
SALMETROL-FLUTICASON 500/50 DISK INH	ADVAIR 500/50 DISK INH	13
SCOPOLAMINE 0.25% OPTH DROP	ISOPTO HYOSCIN 0.25% OPTH	22
SELENIUM 2.5% LOTION SHAMPOO	SELSUN 2.5% LOTION SHAMPOO	27
SERTRALINE 50MG TAB	ZOLOFT 50MG TAB	18
SERTRALINE HCL 100MG TAB	ZOLOFT 100MG TAB	18
SILVER SULFADIAZINE 1% CREAM	SSD 1% CREAM	27
SIMVASTATIN 5MG TAB	ZOCOR 5MG TAB	15
SIMVASTATIN 10MG TAB	ZOCOR 10MG TAB	15
SIMVASTATIN 20MG TAB	ZOCOR 20MG TAB	15
SIMVASTATIN 40MG TAB	ZOCOR 40MG TAB	15
SIMVASTATIN 80MG TAB	ZOCOR 80MG TAB	15
SOD POLYSTYRENE SULF 15GM	SOD POLYSTYRENE SULF 15GM	20
SODIUM BICARBONATE 650MG TAB	SODIUM BICARBONATE 650MG	23
SODIUM CHLORIDE 5% OPTH DROP	ADSORBONAC 5% OPTH DROP	23
SPIRONOLACTONE 25MG TAB	ALDACTONE 25MG TAB	20
SPIRONOLACTONE/HCTZ 25/25 TAB	ALDACTAZIDE 25/25 TAB	20
STUARTNATAL 1+1 TABLET	STUARTNATAL 1+1 TABLET	28
SUCCIMER 100MG CAP	CHEMET 100MG CAP	24
SUCRALFATE 1GM TAB	CARAFATE 1GM TAB	24
SULFACETAMIDE 10% OPTH DROP	SULAMYD 10% OPTH DROP	21
SULFADIAZINE 500MG TAB	SULFADIAZINE 500MG TAB	12
SULFAMETH 200/TRIMETH 40MG/5ML SUSP	BACTRIM PEDIATRIC ORAL SUSP	12
SULFAMETH 800/TRIMET 160MG TAB	BACTRIM DS TAB	12
SULFASALAZINE 500MG TAB	AZULFIDINE 500MG TAB	12
SULINDAC 150MG TAB	CLINORIL 150MG TAB	16
SULINDAC 200MG TAB	CLINORIL 200MG TAB	16
SUMATRIPTAN 25MG TAB	IMITREX 25MG TAB	19
SUMATRIPTAN 50MG TAB	IMITREX 50MG TAB	19
SUMATRIPTAN 100MG TAB	IMITREX 100MG TAB	19
TAMOXIFEN 10MG TAB	NOLVADEX 10MG TAB	12
TELMISARTAN 40MG TAB	MICARDIS 40MG TAB	16
TELMISARTAN 80MG TAB	MICARDIS 80MG TAB	16
TERBUTALINE 2.5MG TAB	BRETHINE 2.5MG TAB	13
TERBUTALINE 5MG TAB	BRETHINE 5MG TAB	13
TERCONAZOLE VAG 0.4% CREAM	TERAZOL-7 VAG CREAM	26
TERCONAZOLE VAG 0.8% CREAM	TERAZOL-3 VAG CREAM	26
TETRACYCLINE 250MG CAP	SUMYCIN 250MG CAP	11
THEOPHYLLINE 200MG TAB SR	THEODUR 200MG TAB SR	28
THEOPHYLLINE 300MG TAB SR	THEODUR 300MG TAB SR	28
THEOPHYLLINE 80MG/15ML ELIXIR	ELIXOPHYLLIN 80MG/15ML ELIX	28
THIORIDAZINE 100MG TAB	MELLARIL 100MG TAB	18
THIORIDAZINE 25MG TAB	MELLARIL 25MG TAB	18

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
GENERIC TO BRAND

10/30/2006

****

GENERIC NAME	BRAND NAME	PAGE
TIMOLOL 0.5% OPTH DROP	TIMOPTIC 0.5% OPTH DROP	23
TOBRAMYCIN 0.3% EYE OINT	TOBREX 0.3% EYE OINT	21
TOBRAMYCIN 0.3% OPTH DROP	TOBREX 0.3% OPTH DROP	21
TOBRAMYCIN/DEXAMETHA OPTH DROP	TOBRADEX OPTH DROP	21
TOBRAMYCIN/DEXMETHA EYE OINT	TOBRADEX EYE OINT	21
TOLMETIN 400MG DS CAP	TOLECTIN DS 400MG CAP	16
TRIAMCINOLONE 0.1% PASTE	KENALOG IN ORABASE 0.1% P	27
TRIAMTERENE 37.5/HCTZ 25 TAB	MAXZIDE 37.5MG/25MG TAB	20
TRIFLUOPERAZINE 5MG TAB	STELAZINE 5MG TAB	18
TRIFLURIDINE 1% OPTH DROP	VIROPTIC 1% OPTH DROP	21
RIMETHOBENZAMIDE 100MG SUPP	TIGAN 100MG SUPP	24
TRIMETHOBENZAMIDE 200MG SUPP	TIGAN 200MG SUPP	24
TRIMETHOPRIM 100MG TAB	TRIMPEX 100MG TAB	12
TRIMETHOPRIM/POLYMIX OPTH	POLYTRIM OPHTHALMIC DROP	21
TRIPHASIL-28 TAB	TRIPHASIL-28 TAB	25
TROPICAMIDE 1% OPTH DROP	MYDRIACYL 1% OPTH DROP	22
VALPROIC ACID 250MG CAP	DEPAKENE 250MG CAP	17
VASOCON-A OPHTHALMIC DROP	VASOCON-A OPHTHALMIC DROP	23
VERAPAMIL 120MG TAB	CALAN 120MG TAB	15
VERAPAMIL 240MG CAP SA	VERELAN 240MG CAP SA	15
VERAPAMIL 80MG TAB	CALAN 80MG TAB	15
VIT B COMPLX/VIT C/PLUS FE TAB	NEPHRO-VITE PLUS IRON TAB	28
WARFARIN SODIUM 5MG TAB	COUMADIN 5MG TAB	14
WARFARIN SODIUM 2.5MG TAB	COUMADIN 2.5MG TAB	14

**** REPORT COMPLETED ****

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
ACCUZYME TOPICAL OINT	PAPAIN-UREA 1.lMU-100MG/GM OINT	27
ACULAR 0.5% OPTH DROP	KETOROLAC TROM 0.5% OPTH DROP	22
ADALAT CC 30MG TAB	NIFEDIPINE CC 30MG TAB	15
ADALAT CC 60MG TAB	NIFEDIPINE CC 60MG TAB	15
ADALAT CC 90MG TAB	NIFEDIPINE CC 90MG TAB	15
ADSORBONAC 5% OPTH DROP	SODIUM CHLORIDE 5% OPTH DROP	23
ADVAIR 100/50 DISK INH	SALMTROL-FLUTCASON 100/50 DISK INH	13
ADVAIR 250/50 DISK INH	SALMTROL-FLUTCASON 250/50 DISK INH	13
ADVAIR 500/50 DISK INH	SALMTROL-FLUTCASON 500/50 DISK INH	13
ALDACTAZIDE 25/25 TAB	SPIRONOLACTONE/HCTZ 25/25 TAB	20
ALDACTONE 25MG TAB	SPIRONOLACTONE 25MG TAB	20
ALDOMET 250MG TAB	METHYLDOPA 250MG TAB	16
ALKERAN 2MG TAB	MELPHALAN 2MG TAB	12
ALPHAGAN 0.2% OPHTH DROP	BRIMONIDINE 0.2% OPHTH DROP	23
ALUPENT 10MG TAB	METAPROTERENOL 10MG TAB	13
ALUPENT 5% INH SOLUTION	METAPROTERENOL 5% INH SOLUTION	13
ALUPENT METERED INHALER	METAPROTERENOL METERED INHALER	13
AMINOPHYLLINE 200MG TAB	AMINOPHYLLINE 200MG TAB	28
AMOXICILLIN 250MG CAP	AMOXICILLIN 250MG CAP	11
AMOXICILLIN 500MG CAP	AMOXICILLIN 500MG CAP	11
ANUSOL HC 25MG SUPP	HYDROCORTISONE 25MG SUPP	27
ANUSOL-HC 2.5% CREAM	HYDROCORTISONE ACET 2.5% CREAM	27
APRESOLINE 25MG TAB	HYDRALAZINE 25MG TAB	15
APRESOLINE 50MG TAB	HYDRALAZINE 50MG TAB	15
ATARAX 10MG TAB	HYDROXYZINE HCL 10MG TAB	19
ATARAX 10MG/5ML SYRUP	HYDROXYZINE 10MG/5ML SYRUP	19
ATARAX 25MG TAB	HYDROXYZINE HCL 25MG TAB	19
ATIVAN 0.5MG TAB	LORAZEPAM 0.5MG TAB	19
ATIVAN 1MG TAB	LORAZEPAM 1MG TAB	19
ATIVAN 2MG TAB	LORAZEPAM 2MG TAB	19
ATROPINE 1% OPTH DROP	ATROPINE 1% OPTH DROP	22
ATROVENT INHALER	IPRATROPIUM BR INHALER	13
AUGMENTIN 125 SUSP	AMOXICILLIN 125/CLAV 31.2 SUSP	10
AUGMENTIN 250 SUSP	AMOXICILLIN 250/CLAV 62.5 SUSP	11
AUGMENTIN 250MG TAB	AMOXICILLIN 250/CLAV 125 TAB	11
AUGMENTIN 500MG TAB	AMOXICILLIN 500/CLAV 125 TAB	11
AUGMENTIN 875MG TAB	AMOXICILLIN 875/CLAV 125 TAB	11
AURALGAN EAR DROP	AURALGAN EAR DROP	22
AVANDIA 2MG TAB	ROSIGLITAZONE 2MG TAB	25
AVANDIA 4MG TAB	ROSIGLITAZONE 4MG TAB	25
AVANDIA 8MG TAB	ROSIGLITAZONE 8MG TAB	25
AZULFIDINE 500MG TAB	SULFASALAZINE 500MG TAB	12
BACITRACIN 500U/GM EYE OINT	BACITRACIN 500U/GM EYE OINT	21
BACTRIM DS TAB	SULFAMETH 800/TRIMET 160MG/5ML TAB	12
BACTRIM PEDIATRIC ORAL SUSP	SULFAMETH 200/TRIMET 40MG/5ML SUSP	12
BACTROBAN 2% OINT	MUPIROCIN 2% OINT	26
BENADRYL 12.5MG/5ML ELIXIR	DIPHENHYDRAMINE 12.5MG/5ML ELIXIR	10
BENADRYL 25MG CAP	DIPHENHYDRAMINE 25MG CAP	10
BENEMID 500MG TAB	PROBENECID 500MG TAB	21
BENTYL 10MG CAP	DICYCLOMINE 10MG CAP	13

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
BETOPTIC S 0.25% OPTH DROP	BETAXOLOL HCL 0.25% OPTH	23
BIAXIN 250MG TAB	CLARITHROMYCIN 250MG TAB	10
BIAXIN 500MG TAB	CLARITHROMYCIN 500MG TAB	10
BICITRA SUGAR FREE SOLUTION	BICITRA SUGAR FREE SOLUTION	20
BONINE 12.5MG TAB	MECLIZINE HCL 12.5MG TAB	23
BONINE 25MG TAB	MECLIZINE HCL 25MG TAB	23
BRETHINE 2.5MG TAB	TERBUTALINE 2.5MG TAB	13
BRETHINE 5MG TAB	TERBUTALINE 5MG TAB	13
BUMEX 1MG TAB	BUMETANIDE 1MG TAB	20
CAFERGOT TAB	ERGOTAMINE 1MG/CAFF 100MG	14
CALAN 120MG TAB	VERAPAMIL 120MG TAB	15
CALAN 80MG TAB	VERAPAMIL 80MG TAB	15
CALCIUM CARBONATE 650MG TAB	CALCIUM CARBONATE 650MG TAB	20
CAPOTEN 12.5MG TAB	CAPTOPRIL 12.5MG TAB	14
CAPOTEN 25MG TAB	CAPTOPRIL 25MG TAB	14
CARAFATE 1GM TAB	SUCRALFATE 1GM TAB	24
CARDIZEM 30MG TAB	DILTIAZEM 30MG TAB	14
CARDIZEM 60MG TAB	DILTIAZEM 60MG TAB	14
CARDURA 1MG TAB	DOXAZOSIN MESYLATE 1MG TAB	15
CARDURA 2MG TAB	DOXAZOSIN MESYLATE 2MG TAB	15
CARDURA 4MG TAB	DOXAZOSIN MESYLATE 4MG TAB	15
CATAPRES 0.1MG TAB	CLONIDINE HCL 0.1MG TAB	15
CATAPRES 0.2MG TAB	CLONIDINE HCL 0.2MG TAB	15
CATAPRES 0.3MG TAB	CLONIDINE HCL 0.3MG TAB	15
CATAPRES-TTS 1 PATCH	CLONIDINE-TTS 1 PATCH	15
CATAPRES-TTS 2 PATCH	CLONIDINE-TTS 2 PATCH	15
CATAPRES-TTS 3 PATCH	CLONIDINE-TTS 3 PATCH	15
CEPHULAC 10GM/15ML SYRUP	LACTULOSE 10GM/15ML SYRUP	20
CERUMENEX 10% EAR DROP	CERUMENEX 10% EAR DROP	23
CETACAINE 56GM SPRAY	CETACAINE 56GM SPRAY	27
CHEMET 100MG CAP	SUCCIMER 100MG CAP	24
CILOXAN 0.3% EYE OINT	CIPROFLOXACIN 0.3% EYE OINT	21
CILOXAN 0.3% OPTH DROP	CIPROFLOXACIN 0.3% OPTH DRP	21
CIPRO 250MG TAB	CIPROFLOXACIN HCL 250MG TAB	12
CIPRO 500MG TAB	CIPROFLOXACIN HCL 500MG TAB	12
CIPRO 750MG TAB	CIPROFLOXACIN HCL 750MG TAB	12
CLARITIN 10MG TAB	LORATADINE 10MG TAB	10
CLARITIN 5MG/5ML SYRUP	LORATADINE 5MG/5ML SYRUP	10
CLEOCIN 150MG CAP	CLINDAMYCIN 150MG CAP	11
CLEOCIN T 1% SOLUTION	CLINDAMYCIN T 1% SOLUTION	26
CLINORIL 150MG TAB	SULINDAC 150MG TAB	16
CLINORIL 200MG TAB	SULINDAC 200MG TAB	16
CODEINE 30MG TAB	CODEINE SULFATE 30MG TAB	16
COGENTIN 1MG TAB	BENZTROPINE 1MG TAB	13
COGENTIN 2MG TAB	BENZTROPINE 2MG TAB	13
COLCHICINE 0.6MG TAB	COLCHICINE 0.6MG TAB	28
COLY-MYCIN S OTIC DROP	COLY-MYCIN S OTIC DROP	21
COLYTE SOLUTION 4000ML	COLYTE SOLUTION 4000ML	23
COMBIVENT INHALER	ALBUTEROL/IPRATROPIUM INH	13
COMPAZINE 25MG SUPP	PROCHLORPERAZINE 25MG SUPP	24

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
COMPAZINE 5MG TAB	PROCHLORPERAZINE 5MG TAB	24
CONDOMS LUBRICATED/SPERMICIDAL	CONDOMS LUBRICATED/SPERMICIDAL	19
CORDARONE 200MG TAB	AMIODARONE 200MG TAB	14
CORTENEMA 100MG ENEMA	HYDROCORTISONE 100MG ENEMA	27
CORTISPORIN OTIC SUSP	NEOMYC/POLYM B/HC OTIC SUSP	21
COTAZYM CAP	PANCRELIPASE CAP	23
COUMADIN 2.5MG TAB	WARFARIN SODIUM 2.5MG TAB	14
COUMADIN 5MG TAB	WARFARIN SODIUM 5MG TAB	14
CUPRIMINE 250MG CAP	PENICILLAMINE 250MG CAP	24
CYCLOGYL 1% OPTH DROP	CYCLOPENTOLATE 1% OPTH DROP	22
CYCLOMYDRIL OPTH SOLUTION	CYCLOPENTOL/PHENYLEPH OPTH SOL	22
CYTOMEL 25MCG TAB	LIOTHYRONINE 25MCG TAB	26
DALMANE 15MG CAP	FLURAZEPAM 15MG CAP	19
DAPSONE 100MG TAB	DAPSONE 100MG TAB	12
DAPSONE 25MG TAB	DAPSONE 25MG TAB	12
DARAPRIM 25MG TAB	PYRIMETHAMINE 25MG TAB	11
DECADRON 0.5MG TAB	DEXAMETHASONE 0.5MG TAB	24
DECADRON 4MG TAB	DEXAMETHASONE 4MG TAB	24
DELFEN FOAM 12.5% VAGINAL	DELFEN FOAM 12.5% VAGINAL	19
DELTASONE 20MG TAB	PREDNISONE 20MG TAB	24
DELTASONE 5MG TAB	PREDNISONE 5MG TAB	24
DEMEROL 50MG TAB	MEPERIDINE 50MG TAB	16
DEPAKENE 250MG CAP	VALPROIC ACID 250MG CAP	17
DIAMOX 250MG TAB	ACETAZOLAMIDE 250MG TAB	22
DIAMOX SEQUELS 500MG CAP	ACETAZOLAMIDE 500MG CAP	22
DIDRONEL 200MG TAB	ETIDRONATE 200MG TAB	28
DIFLUCAN 150MG TAB	FLUCONAZOLE 150MG TAB	10
DILANTIN 100MG CAP	PHENYTOIN 100MG CAP	17
DILANTIN 125MG/5ML SUSP	PHENYTOIN 125MG/5ML SUSP	17
DILANTIN 50MG TAB	PHENYTOIN 50MG TAB	17
DILANTIN 30MG SR CAP	PHENYTOIN SOD 30MG SR CAP	17
DILAUDID 2MG TAB	HYDROMORPHONE 2MG TAB	16
DITROPAN 5MG TAB	OXYBUTYNIN 5MG TAB	27
DIULO 5MG TAB	METOLAZONE 5MG TAB	20
DULCAGEN 10MG SUPP	BISACODYL 10MG SUPP	23
E.E.S 250MG FILMTAB	ERYTHROMYCIN 250MG FILMTAB	10
E.E.S. 200MG/5ML SUSP	ERYTHROMYCIN 200MG/5ML SUSP	10
ELAVIL 10MG TAB	AMITRIPTYLINE 10MG TAB	18
ELAVIL 25MG TAB	AMITRIPTYLINE 25MG TAB	18
ELAVIL 50MG TAB	AMITRIPTYLINE HCL 50MG TAB	18
ELIMITE 5% CREAM	PERMETHRIN 5% CREAM	26
ELIXOPHYLLIN 80MG/15ML ELIXIR	THEOPHYLLINE 80MG/15ML ELIXIR	28
ESIDREX 25MG TAB	HYDROCHLOROTHIAZIDE 25MG TAB	20
ESIDREX 50MG TAB	HYDROCHLOROTHIAZIDE 50MG TAB	20
ESKALITH 300MG CAP	LITHIUM CARBONATE 300MG CAP	19
FELDENE 10MG CAP	PIROXICAM 10MG CAP	16
FELDENE 20MG CAP	PIROXICAM 20MG CAP	16
FERROUS SULF 325MG TAB UD	FERROUS SULF 325MG TAB UD	14
FERROUS SULF 220MG/5ML ELIXIR	FERROUS SUL 220MG/5ML ELIXIR	14
FIORINAL TAB	BUTALB 50/CAFF 40/ASA 325 TAB	16
FLAGYL 250MG TAB	METRONIDAZOLE 250MG TAB	12

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
FLEXERIL 10MG TAB	CYCLOBENZAPRINE 10MG TAB	14
FLORINEF 0.1MG TAB	FLUDROCORTISONE 0.1MG TAB	24
FLOVENT 110MCG INHALER	FLUTICASONE PROPIO 110 INH	24
FLOVENT 44MCG INHALER	FLUTICASONE PROPION 44 INH	24
FLOXIN OTIC 0.3% DROP	OFLOXACIN OTIC 0.3% DROP	21
FML EYE OINT	FLUOROMETHOLONE EYE OINT	22
FOLIC ACID 1MG TAB	FOLIC ACID 1MG TAB	28
GARAMYCIN 0.1% TOPICAL CREAM	GENTAMICIN 0.1% TOPICAL CR	26
GARAMYCIN 3MG/ML OPTH DROP	GENTAMICIN 3MG/ML OPTH DROP	21
GARAMYCIN EYE OINT	GENTAMICIN SULF EYE OINT	21
GASTROGRAFFIN SOLUTION	GASTROGRAFFIN SOLUTION	19
GLUCOPHAGE 500MG TAB	METFORMIN HCL 500MG TAB	25
GLUCOPHAGE 850MG TAB	METFORMIN HCL 850MG TAB	25
GLUCOPHAGE XR 500MG TAB	METFORMIN XR 500MG TAB	25
GLUCOTROL 5MG TAB	GLIPIZIDE 5MG TAB	25
GONIOSOL 2.5% OPTH SOLUTION	HYDROXYPROPYLMETH 2.5% OPTH	23
GRANULEX SPRAY	GRANULEX SPRAY	21
GRIFULVIN V 125MG/5ML SUSP	GRISEOFULVIN 125MG/5ML SUSP	10
GRIFULVIN V 250MG TAB	GRISEOFULVIN 250MG TAB	10
HALDOL 1MG TAB	HALOPERIDOL 1MG TAB	18
HALDOL 5MG TAB	HALOPERIDOL 5MG TAB	18
HYDREA 500MG CAP	HYDROXYUREA 500MG CAP	12
HYDROCORTISONE 1% CREAM	HYDROCORTISONE 1% CREAM	27
HYDROCORTISONE 1% OINT	HYDROCORTISONE 1% OINT	27
HYPOTEARS OPTH DROP	HYPOTEARS OPTH DROP	23
ILOTYCIN EYE OINT	ERYTHROMYCIN EYE OINT	21
IMDUR 120MG TAB CR	ISOSORBIDE MONONIT 120MG	16
IMDUR 30MG TAB CR	ISOSORBIDE MONONIT 30MG TAB	16
IMDUR 60MG TAB CR	ISOSORBIDE MONONIT 60MG TAB	16
IMITREX 25MG TAB	SUMATRIPTAN 25MG TAB	19
IMITREX 50MG TAB	SUMATRIPTAN 50MG TAB	19
IMITREX 100MG TAB	SUMATRIPTAN 100MG TAB	19
IMODIUM 2MG CAP	LOPERAMIDE 2MG CAP	23
IMURAN 50MG TAB	AZATHIOPRINE 50MG TAB	28
INDERAL 10MG TAB	PROPRANOLOL 10MG TAB	15
INDERAL 40MG TAB	PROPRANOLOL 40MG TAB	15
INDERAL LA 120MG CAP	PROPRANOLOL LA 120MG CAP	15
INDERAL LA 160MG CAP	PROPRANOLOL LA 160MG CAP	15
INDERAL LA 80MG CAP	PROPRANOLOL LA 80MG CAP	15
INDOCIN 25MG CAP	INDOMETHACIN 25MG CAP	16
INSULIN 1ML U-100 SYRINGE	INSULIN 1ML U-100 SYRINGE	28
ISONIAZID 100MG TAB	ISONIAZID 100MG TAB	11
ISONIAZID 300MG TAB	ISONIAZID 300MG TAB	11
ISONIAZID 50MG/5ML SYRUP	ISONIAZID 50MG/5ML SYRUP	11
ISOPTO HOMATROPIN 2% OPTH SUSP	HOMATROPINE 2% OPTH DROP	22
ISOPTO HOMATROPIN 5% OPTH SUSP	HOMATROPINE 5% OPTH DROP	22
ISOPTO HYOSCIN 0.25% OPTH SUSP	SCOPOLAMINE 0.25% OPTH DROP	22
KEFLEX 125MG/5ML ORAL SUSP	CEPHALEXIN 125MG/5ML ORAL	10
KEFLEX 250MG CAP	CEPHALEXIN 250MG CAP	10

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
KEFLEX 500MG CAP	CEPHALEXIN 500MG CAP	10
KENALOG IN ORABASE 0.1% PASTE	TRIAMCINOLONE 0.1% PASTE	27
KLONOPIN 0.5MG TAB	CLONAZEPAM 0.5MG TAB	17
KLONOPIN 1MG TAB	CLONAZEPAM 1MG TAB	17
KLONOPIN 2MG TAB	CLONAZEPAM 2MG TAB	17
KLOR 20MEQ PKT	POTASSIUM CHLORIDE 20MEQ	20
KLORVESS 20MEQ TAB	POTASSIUM CHLORIDE 20MEQ	20
LACRILUBE S.O.P. EYE OINT	LACRILUBE EYE OINT	23
LAMICTAL 100MG TAB	LAMOTRIGINE 100MG TAB	17
LAMICTAL 25MG TAB	LAMOTRIGINE 25MG TAB	17
LANOXIN 0. 05MG/ML ELIXIR	DIGOXIN 0.05MG/ML ELIXIR	14
LANOXIN 0.125MG TAB	DIGOXIN 0.125MG TAB	14
LANOXIN 0.25MG TAB	DIGOXIN 0.25MG TAB	14
LANTUS 100U/ML VIAL	INSULIN GLARGINE 100U/ML VL	25
LASIX 20MG TAB	FUROSEMIDE 20MG TAB	20
LASIX 40MG TAB	FUROSEMIDE 40MG TAB	20
LCD 5% IN AQUAPHOR	LCD 5% IN AQUAPHOR	27
LEDERCILLIN VK 250MG/5ML SUSP	PENICILLIN VK 250MG/5ML	11
LEUKERAN 2MG TAB	CHLORAMBUCIL 2MG TAB	12
LEVAQUIN 250 MG TAB	LEVOFLOXACIN 250MG TAB	12
LEVAQUIN 500 MG TAB	LEVOFLOXACIN 250MG TAB	12
LEVAQUIN 750 MG TAB	LEVOFLOXACIN 250MG TAB	12
LEVOTHROID 0.025MG TAB	LEVOTHYROXINE 0.025MG TAB	25
LIBRIUM 10MG CAP	CHLORDIAZEPOXIDE 10MG CAP	18
LIBRIUM 25MG CAP	CHLORDIAZEPOXIDE 25MG CAP	18
LIBRIUM 5MG CAP	CHLORDIAZEPOXIDE 5MG CAP	18
LIDOCAINE 2% VISCOUS SOLUTION	LIDOCAINE 2% VISCOUS SOL	22
LIORESAL 10MG TAB	BACLOFEN 10MG TAB	14
LIPITOR 80MG TAB	ATORVASTATIN 80MG TAB	15
LO/OVRAL-28 TAB	LO/OVRAL-28 TAB	24
LOMOTIL TAB	DIPHENOXYLATE/ATROPINE TAB	23
LONITEN 10MG TAB	MINOXIDIL 10MG TAB	16
LONITEN 2.5MG TAB	MINOXIDIL 2.5MG TAB	16
LOPRESSOR 50MG TAB	METOPROLOL 50MG TAB	15
LUGOLS SOLUTION	LUGOLS SOLUTION	21
MAALOX EXTRA STRENGTH LIQ	MAALOX EXTRA STRENGTH	23
MACRODANTIN 100MG CAP	NITROFURANTOIN 100MG CAP	12
MACRODANTIN 50MG CAP	NITROFURANTOIN 50MG CAP	12
MAGIC MOUTHWASH SOL	MAGIC MOUTHWASH SOL	22
MAXIFLOR 0.05% CR	DIFLORASONE 0.05% CREAM	27
MAXIFLOR 0.05% OINT	DIFLORASONE 0.05% OINT	27
MAXITROL OPTHALMIC DROP	MAXITROL OPTHALMIC DROP	21
MAXZIDE 37.5MG/25MG TAB	TRIAMTERENE 37.5/HCTZ 25	20
MEDROL 4MG DOSEPAK	METHYLPREDNISOLONE 4MG DOSE	24
MEDROL 4MG TAB	METHYLPREDNISOLONE 4MG TAB	24
MEGACE 40MG TAB	MEGESTROL 40MG TAB	12
MEGACE 40MG/ML ORAL SUSP	MEGESTROL 40MG/ML ORAL SUSP	12

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
MELLARIL 100MG TAB	THIORIDAZINE 100MG TAB	18
MELLARIL 25MG TAB	THIORIDAZINE 25MG TAB	18
MENTHOL 1/4% IN AQUAPHOR	MENTHOL 1/4% IN AQUAPHOR	27
MEPHYTON 5MG TAB	PHYTONADIONE 5MG TAB	28
MESTINON 60MG TAB	PYRIDOSTIGMINE 60MG TAB	13
METHERGINE 0.2MG TAB	METHYLERGONOVINE 0.2MG TAB	26
METHOTREXATE 2.5MG TAB	METHOTREXATE 2.5MG TAB	12
MICARDIS 40MG TAB	TELMISARTAN 40MG TAB	16
MICARDIS 80MG TAB	TELMISARTAN 80MG TAB	16
MICRONASE 5MG TAB	GLYBURIDE 5MG TAB	25
MICRONOR 0.35MG TAB	NORETHINDRONE 0.35MG TAB	24
MONOPRIL 10MG TAB	FOSINOPRIL SODIUM 10MG TAB	14
MONOPRIL 20MG TAB	FOSINOPRIL SODIUM 20MG TAB	14
MONOPRIL 40MG TAB	FOSINOPRIL SODIUM 40MG TAB	15
MOTRIN 400MG TAB	IBUPROFEN 400MG TAB	16
MOTRIN 600MG TAB	IBUPROFEN 600MG TAB	16
MS CONTIN 30MG SA TAB	MORPHINE SULFATE 30MG SA	17
MYAMBUTOL 100MG TAB	ETHAMBUTOL 100MG TAB	11
MYAMBUTOL 400MG TAB	ETHAMBUTOL 400MG TAB	11
MYCELEX 10MG TROCHE	CLOTRIMAZOLE 10MG TROCHE	26
MYCITRACIN OINT	NEOMYCI/BACITRACI/POLYMIX	26
MYDRIACYL 1% OPTH DROP	TROPICAMIDE 1% OPTH DROP	22
MYLERAN 2MG TAB	BUSULFAN 2MG TAB	12
MYSOLINE 250MG TAB	PRIMIDONE 250MG TAB	17
NAPROSYN 250MG TAB	NAPROXEN 250MG TAB	16
NAPROSYN 375MG TAB	NAPROXEN 375MG TAB	16
NASALIDE 0.025% NASAL INH	FLUNISOLIDE 0.025% NASAL	22
NEOSYNEPHRINE 2.5% OPTH DROP	PHENYLEPHRINE 2.5% OPTH DRP	23
NEPHRO-VITE PLUS IRON TAB	VIT B COMPLX/VIT C/PLUS FE	28
NEPTAZANE 50MG TAB	METHAZOLAMIDE 50MG TAB	22
NEURONTIN 300MG CAP	GABAPENTIN 300MG CAP	17
NEURONTIN 400MG CAP	GABAPENTIN 400MG CAP	17
NILSTAT 100000U/GM CREAM	NYSTATIN 100000U/GM CREAM	26
NILSTAT 100000U/GM OINT	NYSTATIN 100000U/GM OINT	26
NILSTAT 100000U/ML SUSP	NYSTATIN 100000U/ML SUSP	10
NITRO-DUR 0.4MG/HR PATCH	NITROGLYCERIN 0.4MG/HR PAT	16
NITROL 2% OINT	NITROGLYCERIN 2% OINT	16
NITROSTAT 0.4MG TAB SL	NITROGLYCERIN 0.4MG TAB SL	16
NITROSTAT 0.6MG TAB SL	NITROGLYCERIN 0.6MG TAB SL	16
NIX 1% CREME RINSE LIQUID	PERMETHRIN 1% CREME RINSE	26
NIZORAL 2% CREAM	KETOCONAZOLE 2% CREAM	26
NOLVADEX 10MG TAB	TAMOXIFEN 10MG TAB	12
NORDETTE-28 TAB	NORDETTE-28 TAB	24
NORMODYNE 100MG TAB	LABETALOL 100MG TAB	15
NORMODYNE 200MG TAB	LABETALOL 200MG TAB	16
NORPRAMIN 10MG TAB	DESIPRAMINE 10MG TAB	18
NORPRAMIN 50MG TAB	DESIPRAMINE 50MG TAB	18
NORPRAMINE 25MG TAB	DESIPRAMINE 25MG TAB	18
NORVASC 10MG TAB	AMLODIPINE BESYLATE 10MG	14
NORVASC 5MG TAB	AMLODIPINE BESYLATE 5MG TAB	14

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
NOVOLIN 70/30 100U/ML VIAL	INSULIN HUMAN SEMISYNTH 70/30U	25
NOVOLIN LENTE 100U/ML VIAL	INSULIN HUMAN SEMISY L 100U/ML	25
NOVOLIN NPH 100U/ML VIAL	INSULIN HUMAN SEMI NPH 10OU/ML	25
NOVOLIN REGULAR 100U/ML VIAL	INSULIN HUMAN SEMISY R 10OU/ML	25
OPHTHETIC 0.5% OPTH DROP	PROPARACAINE 0.5% OPTH DROP	22
ORTHO-DIAPHRAGM ALLFLX 65	DIAPHRAGM ARC-SPRING 65MM	19
ORTHO-DIAPHRAGM ALLFLX 70	DIAPHRAGM ARC-SPRING 70MM	19
ORTHO-DIAPHRAGM ALLFLX 75	DIAPHRAGM ARC-SPRING 75MM	19
ORTHO-DIAPHRAGM ALLFLX 80	DIAPHRAGM ARC-SPRING 80MM	19
ORTHO-DIAPHRAGM ALLFLX 85	DIAPHRAGM ARC-SPRING 85MM	19
ORTHO EVRA PATCH	ORTHO EVRA PATCH	24
ORTHO NOVUM-1/35 28 DAY	ORTHO NOVUM-1/35 28 DAY TAB	24
ORTHO NOVUM-777 28 DAY TAB	ORTHO NOVUM-777 28 DAY TAB	25
ORTHO-NOVUM 1/50 28 DAY TAB	ORTHO-NOVUM 1/50 28 DAY TAB	25
ORUDIS 50MG CAP	KETOPROFEN 50MG CAP	16
PAMELOR 10MG CAP	NORTRIPTYLINE HCL 10MG CAP	18
PAMELOR 25MG CAP	NORTRIPTYLINE HCL 25MG CAP	18
PAREGORIC LIQ	PAREGORIC LIQ	23
PARLODEL 2.5MG TAB	BROMOCRIPTINE 2.5MG TAB	28
PATHOCIL 250MG CAP	DICLOXACILLIN 250MG CAP	11
PEDIAZOLE ORAL SUSP	ERYTHROMYCIN/SULFISOX SUSP	12
PENICILLIN VK 250MG TAB	PENICILLIN VK 250MG TAB	11
PERCOCET 5/325MG TAB	OXYCODONE 5/ACETAMIN 325MG TAB	17
PERSANTINE 25MG TAB	DIPYRIDAMOLE 25MG TAB	16
PHENERGAN 25MG SUPP	PROMETHAZINE HCL 25MG SUPP	10
PHENERGAN 50MG SUPP	PROMETHAZINE HCL 50MG SUPP	10
HENOBARBITAL 20MG/5ML ELIXIR	PHENOBARBITAL 20MG/5ML ELIXIR	18
PHENOBARBITAL 30MG TAB	PHENOBARBITAL 30MG TAB	18
PILOCAR 2% OPTH DROP	PILOCARPINE 2% OPTH DROP	22
PILOCAR 4% OPTH DROP	PILOCARPINE 4% OPTH DROP	22
PILOPINE HS 4% EYE GEL	PILOCARPINE 4% EYE GEL	22
PLAQUENIL 200MG TAB	HYDROXYCHLOROQUINE 200MG TAB	11
PLAVIX 75MG TAB	CLOPIDOGREL 75MG TAB	28
POLYTRIM OPHTHALMIC DROP	TRIMETHOPRIM/POLYMIX OPTH DROP	21
POTASSIUM CHLORIDE 10% SOLUTION	POTASSIUM CHLORIDE 10% SOL	20
PRED FORTE 1% OPTH DROP	PREDNISOLONE ACET 1% OPTH	22
PREDNISONE 5MG/5ML ORAL SOLUTION	PREDNISONE 5MG/5ML ORAL SOL	24
PREMARIN 0.625MG TAB	ESTROGENS, CONJ 0.625MG TAB	25
PREMARIN 1.25MG TAB	ESTROGENS, CONJ 1.25MG TAB	25
PREMARIN VAG CR W/APP	ESTROGENS, CONJ VAG CR W/ APP	25
PREMPRO 2.5MG TAB	CONJ ESTROG/MEDROXYPROG 2.5 TAB	25
PRILOSEC OTC 20MG TAB 14’s	OMEPRAZOLE OTC 20MG TAB 14’s	24
PRILOSEC OTC 20MG TAB 28’s	OMEPRAZOLE OTC 20MG TAB 28’s	24
PRIMAQUINE 26.3MG TAB	PRIMAQUINE 26.3MG TAB	11
PROBANTHINE 15MG TAB	PROPANTHELINE 15MG TAB	13
PROCAN 250MG CAP	PROCAINAMIDE 250MG CAP	15
PROCAN SR 500MG TAB	PROCAINAMIDE SR 500MG TAB	15
PROCARDIA 10MG CAP	NIFEDIPINE 10MG CAP	15
PROLIXIN 1MG TAB	FLUPHENAZINE HCL 1MG TAB	18
PROLIXIN 5MG TAB	FLUPHENAZINE 5MG TAB	18

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
PROPINE 0.1% OPTH DROPS	DIPIVEFRIN 0.1% OPTH DROP	22
PROPYLTHIOURACIL 50MG TAB	PROPYLTHIOURACIL 50MG TAB	26
PROVENTIL 2MG TAB	ALBUTEROL 2MG TAB	13
PROVENTIL 2MG/5ML SYRUP	ALBUTEROL 2MG/5ML SYRUP	13
PROVENTIL 4MG REPETAB	ALBUTEROL 4MG REPETAB	13
PROVENTIL 4MG TAB	ALBUTEROL 4MG TAB	13
PROVENTIL METERED INHALER	ALBUTEROL METERED INHALER	13
PROVENTIL 0.083% NEB UD SOL	PROVENTIL 0.083% NEB UD SOL	13
PROVERA 10MG TAB	MEDROXYPROGESTERONE 10MG	25
PULMICORT REPULES 0.25MG INH SUSP	BUDESONIDE 0.25MG INH SUSP	24
** Restriction: Patient less than 4 years old **		
PULMICORT REPULES 0.5MG INH SUSP	BUDESONIDE 0.5MG INH SUSP	24
** Restriction: Patient less than 4 years old **		
PYRAZINAMIDE 500MG TAB	PYRAZINAMIDE 500MG TAB	11
PYRIDIUM 100MG TAB	PHENAZOPYRIDINE 100MG TAB	27
QUESTRAN LIGHT PKT	CHOLESTYRAMINE LIGHT PKT	15
QUINAGLUTE 324MG TAB	QUINIDINE GLUCONATE 324MG TAB	15
QUINORA 200MG TAB	QUINIDINE SULFATE 200MG TAB	15
REGLAN 5MG/5ML SYRUP	METOCLOPRAMIDE 5MG/5ML SYRUP	24
REGLAN 10MG TAB	METOCLOPRAMIDE 10MG TAB	24
RID LIQUID	PIPERONYL/PYRETHRIN LIQUID	26
RIDAURA 3MG CAP	AURANOFIN 3MG CAP	24
RIMACTANE 300MG CAP	RIFAMPIN 300MG CAP	11
RITALIN 10MG TAB	METHYLPHENIDATE 10MG TAB	18
ROBITUSSIN AC SYRUP	GUAIFENSIN/CODEINE SYRUP	21
ROCALTROL 0.25MCG CAP	CALCITRIOL 0.25MCG CAP	28
RONDEC DM DROP	PSEUDOEPHED/CARBINOX DM DROP	21
RONDEC DM SYRUP	PSEUDOEPHED/CARBINOX DM SYRUP	21
ROXANOL 20MG/ML SOLUTION	MORPHINE SULFATE 20MG/ML SOL	17
ROXANOL 20MG/ML-12-ML SOLUTION	MORPHINE SUL 20MG/ML-120ML SOL	17
SALICYLIC ACID 5% IN AQUAPHOR	SALICYLIC ACID 5% IN AQUAPHOR	27
SANDIMMUNE 100MG/ML SOLUTION	CYCLOSPORINE 100MG/ML SOL	28
SELSUN 2.5% LOTION SHAMPOO	SELENIUM 2.5% LOTION SHAMPOO	27
SEREVENT DISKUS 50MCG INH	SALMETEROL DISKUS 50MCG INH	13
SINEMET-10/100 TAB	CARBIDOPA/LEVODOPA 10/100 TAB	19
SINEMET-25/100 TAB	CARBIDOPA/LEVODOPA 25/100 TAB	19
SINEMET-25/250 TAB	CARBIDOPA/LEVODOPA 25/250 TAB	19
SINGULAIR 10MG TAB	MONTELKAST 10MG TAB	28
SINGULAIR 5MG CHEW TAB	MONTELKAST 5MG CHEW TAB SOD	28
SODIUM BICARBONATE 650MG TAB	SODIUM BICARBONATE 650MG TAB	23
SOD POLYSTYRENE SULF 15GM	SOD POLYSTYRENE SULF 15GM	20
SPECTAZOLE 1% TOPICAL CREAM	ECONAZOLE 1% TOPICAL CREAM	26
SSD 1% CREAM	SILVER SULFADIAZINE 1% CREAM	27
STELAZINE 5MG TAB	TRIFLUOPERAZINE 5MG TAB	18
STUARTNATAL 1+1 TABLET	STUARTNATAL 1+1 TABLET	28
SULAMYD 10% OPTH DROP	SULFACETAMIDE 10% OPTH DROP	21
SULFADIAZINE 500MG TAB	SULFADIAZINE 500MG TAB	12
SUMYCIN 250MG CAP	TETRACYCLINE 250MG CAP	11
SYNEMOL 0.025% CREAM	FLUOCINOLONE ACETONI 0.02 CREAM	27
SYNTHROID 0.05MG TAB	LEVOTHYROXINE 0.05MG TAB	25

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
SYNTHROID 0.075MG TAB	LEVOTHYROXINE 0.075MG TAB	26
SYNTHROID 0.125MG TAB	LEVOTHYROXINE 0.125MG TAB	26
SYNTHROID 0.15MG TAB	LEVOTHYROXINE 0.15MG TAB	26
SYNTHROID 0.1MG TAB	LEVOTHYROXINE 0.1MG TAB	26
TEGRETOL 100MG TAB	CARBAMAZEPINE 100MG TAB	17
TEGRETOL 100MG/5ML SUSP	CARBAMAZEPINE 100MG/5ML SUS	17
TEGRETOL 200MG TAB	CARBAMAZEPINE 200MG TAB	17
TEN-K 10MEQ SA TAB	POTASSIUM CL 10MEQ SA TAB	20
TENORMIN 50MG TAB	ATENOLOL 50MG TAB	14
TERAZOL-3 VAG 0.8% CREAM	TERCONAZOLE VAG 0.8% CREAM	26
TERAZOL-7 VAG CREAM	TERCONAZOLE VAG 0.4% CREAM	26
THEODUR 200MG TAB SR	THEOPHYLLINE 200MG TAB SR	28
THEODUR 300MG TAB SR	THEOPHYLLINE 300MG TAB SR	28
THORAZINE 25MG TAB	CHLORPROMAZINE 25MG TAB	18
THORAZINE 50MG TAB	CHLORPROMAZINE 50MG TAB	18
TIAZAC 180MG CR CAP	DILTIAZEM 180MG CR CAP	14
TIAZAC 240MG CR CAP	DILTIAZEM HCL 240MG CR CA	14
TIAZAC 300MG CR CAP	DILTIAZEM HCL 300MG CR CA	14
TIGAN 100MG SUPP	TRIMETHOBENZAMIDE 100MG SUPP	24
TIGAN 200MG SUPP	TRIMETHOBENZAMIDE 200MG SUPP	24
TIMOPTIC 0.5% OPTH DROP	TIMOLOL 0.5% OPTH DROPS	23
TOBRADEX EYE OINT	TOBRAMYCIN/DEXMETHA EYE O	21
TOBRADEX OPTH DROP	TOBRAMYCIN/DEXAMETHA OPTH	21
TOBREX 0.3% EYE OINT	TOBRAMYCIN 0.3% EYE'OINT	21
TOBREX 0.3% OPTH DROP	TOBRAMYCIN 0.3% OPTH DROP	21
TOFRANIL 10MG TAB	IMIPRAMINE HCL 10MG TAB	18
TOFRANIL 25MG TAB	IMIPRAMINE 25MG TAB	18
TOLECTIN DS 400MG CAP	TOLMETIN 400MG DS CAP	16
TRANSDERM-NITRO 0.2MG/HR PATCH	NITROGLYCERIN 0.2MG/HR PA	16
TRENTAL 400MG TAB SA	PENTOXIFYLLINE 400MG TAB	14
TRIMOX 125/5ML SUSP	AMOXICILLIN 125MG/5ML SUSP	10
TRIMOX 250MG/5ML SUSP	AMOXICILLIN 250MG/5ML SUSP	11
TRIMPEX 100MG TAB	TRIMETHOPRIM 100MG TAB	12
TRIPHASIL-28 TAB	TRIPHASIL-28 TAB	25
TRUSOPT 2% OPTH DROP	DORZOLAMIDE HCL 2% OPTH DROP	22
TYLENOL 100MG/ML DROP	ACETAMINOPHEN 100MG/ML DROP	17
TYLENOL 160MG/5ML ELXILIR	ACETAMINOPHEN 160MG/5ML ELX	17
TYLENOL W/ CODEINE NO.3 TAB	ACETAMINO 300/CODEINE 30MG	16
TYLENOL W/CODEINE ELIXIR	ACETAMINO 120/COD 12MG/5ML	16
URECHOLINE 10MG TAB	BETHANECOL 10MG TAB	13
URECHOLINE 25MG TAB	BETHANECHOL 25MG TAB	13
URECHOLINE 5MG TAB	BETHANECHOL 5MG TAB	13
VALIUM 5MG TAB	DIAZEPAM 5MG TAB	19
VANCERIL INHALER	BECLOMETHASONE INHALER	24
VASOCON-A OPHTHALMIC DROP	VASOCON-A OPHTHALMIC DROP	23
VERELAN 240MG CAP SA	VERAPAMIL 240MG CAP SA	15
VERMOX 100MG CHEWABLE TAB	MEBENDAZOLE 100MG CHEWABLE	10
VIBRAMYCIN 100MG CAP	DOXYCYCLINE 100MG CAP	11
VIROPTIC 1% OPTH DROP	TRIFLURIDINE 1% OPTH DROP	21
VITAMIN B-6 50MG TAB	PYRIDOXINE 50MG TAB	28

DISTRICT OF COLUMBIA
HEALTHCARE ALLIANCE
BRAND TO GENERIC

10/30/2006

****

BRAND NAME	GENERIC NAME	PAGE
VOSOL 2% OTIC SOL	ACETIC ACID 2% OTIC SOL	22
VOSOL HC OTIC SOL	ACETIC ACID 2%/HC 1% OTIC	22
WELLCOVORIN 25MG TAB	LEUCOVORIN CALCIUM 25MG TAB	28
WELLCOVORIN 5MG TAB	LEUCOVORIN CALCIUM 5MG TAB	28
XALATAN 0.005% OPHTH DROP	LATANOPROST 0.005% OPHTH	23
XANAX 0.25MG TAB	ALPRAZOLAM 0.25MG TAB	18
XANAX 0.5MG TAB	ALPRAZOLAM 0.5MG TAB	18
XANAX 1MG TAB	ALPRAZOLAM 1MG TAB	18
XYLOCAINE 2% JELLY	LIDOCAINE HCL 2% JELLY	22
XYLOCAINE 5% OINT	LIDOCAINE HCL 5% OINT	27
ZANTAC 150MG TAB	RANITIDINE 150MG TAB	24
ZESTRIL 10MG TAB	LISINOPRIL 10MG TAB	15
ZESTRIL 20MG TAB	LISINOPRIL 20MG TAB	15
ZESTRIL 5MG TAB	LISINOPRIL 5MG TAB	15
ZITHROMAX 250MG CAP (Z-PAK)	AZITHROMYCIN 250MG CAP (Z-P)	10
ZITHROMAX 600MG/15ML ORAL SUSP	AZITHROMYCIN 600MG/15ML	10
ZITHROMAX 900MG/22.5ML ORAL SUSP	AZITHROMYCIN 900MG/22.5ML	10
ZOCOR 5MG TAB	SIMVASTATIN 5MG TAB	15
ZOCOR 10MG TAB	SIMVASTATIN 10MG TAB	15
ZOCOR 20MG TAB	SIMVASTATIN 20MG TAB	15
ZOCOR 40MG TAB	SIMVASTATIN 40MG TAB	15
ZOCOR 80MG TAB	SIMVATATTIN 80MG TAB	15
ZOLOFT 100MG TAB	SERTRALINE HCL 100MG TAB	18
ZOLOFT 50MG TAB	SERTRALINE 50MG TAB	18
ZOVIRAX 200MG CAP	ACYCLOVIR 200MG CAP	11
ZOVIRAX 5% OINT	ACYCLOVIR 5% OINT	26
ZYLOPRIM 100MG TAB	ALLOPURINOL 100MG TAB	28
ZYLOPRIM 300MG TAB	ALLOPURINOL 300MG TAB	28

**** REPORT COMPLETED ****

APPENDIX

AIDS DRUG ASSISTANCE PROGRAM FORMULARY...…….. 50
POUND-KILOGRAM CONVERSIONS…….. 51
PHARMACOKINETIC FORMULAS…….. 52
- **A. Ideal Body Weight…….. 52**
- **B. Creatinine Clearance (CrCl)……. 52**
- **C. Creatinine Clearance Values In Renal Dysfunction……... 53**
- **D. Body Surface Area……. 53**

TEMPERATURE CONVERSION…… 53
GLUCOCORTICOID EQUIVALENCIES, POTENCIES, & HALF-LIFE…. 53
APPROXIMATE DOSAGE EQUIVALENTS OF THYROID PRODUCTS.. 54
NARCOTIC AGONISTS (COMPARATIVE PHARMACOKINETICS) ….. 54
GUIDELINE FOR DRUG LEVELS COMMONLY MONITORED…… 55
ADJUSTMENT OF SERUM CONC. WITH LOW SERUM ALBUMIN……. 56
DRUGS WHICH MAY CAUSE DISCOLORATION OF THE FECES……... 56
DRUGS WHICH MAY CAUSE DISCOLORATION OF URINE…… 57
DRUGS WHICH AFFECT LABORATORY VALUES……. 58
REQUEST FOR FORMULARY CHANGE…….……..… 61

ADAP FORMULARY

The following drugs are available through the District of Columbia AIDS Drug Assistance Program.

ANTI-RETROVIRALS

FUSION INHIBITORS
Enfurvirtide (Fuzeon)

NUCLEOSIDE and NUCLEOTIDE REVERSE TRANSCRIPTASE INHIBITORS (NNRTI)
Abacavir (Ziagen)
Abacavir Sulfate/Lamivudine/Zidovudine (Trizivir)
Abacavir/Lamivudine (Epzicom)
Didanosine (Videx)
Emtricitabine (Emtriva)
Lamivudine (3TC, Epivir)
Lamivudine/Zidovudiine (Combivir)
Stavudine (Zerit)
Tenofovir (Viread)
Tenofovir/Emtricitabine (Truvada)
Zalcitabine (HIVID)
Zidovudine (Retrovir, AZT)

NON-NUCLEOSIDE REVERSE TRANSCRIPTASE INHIBITORS (NRTI)
Delaviridine Mesylate (Rescriptor)
Efavirenz (Sustiva)
Nevirapine (Viramune)

PROTEASE INHIBITORS (PI)
Amprenavir (Agenerase)
Atazanavir Sulfate (Reyataz)
Fosamprenavir (Lexiva)
Indinavir (Crixivan)
Lopinavir/Ritonavir (Kaletra)
Nelfinavir (Viracept)
Ritonavir (Norvir)
Saquinavir (Invirase, Fortovase).
Tipranavir (Aptivus)

ADDITIONAL DRUGS

ANALGESICS
Acetaminophen w/ Codeine**
(Tylenol III & Tylenol IV)
Fentanyl (Duragesic) Patch**
Ibuprofen (400mg, 600mg, 800mg)
Morphine Sulfate (MS Contin)**

ANTIBIOTICS
Amoxicillin/Clavulanate
(Augmentin)
Azithromycin (Zithromax)
Ciprofloxacin (Cipro)
Clarithromycin (Biaxin)
Clindamycin HCL (Cleocin)
Doxycycline (Vibramycin)
Ethambutol (Myambutol)
Isoniazid (INH)
Levofloxacin (Levaquin)
Pyrazinamide (Pyrazinamide)
Primethamine (Daraprim)
Rifabutin (Mycobutin)
Rifampin (Rimactane)
Sulfazdiazine

ANTI-CANCER
Alpha-Interferon (Intron A)
Doxorubicin (Doxil)

ANTI-DEPRESSANTS
Amitriptyline HCL (Elavil)
Bupropion (Wellbutrin SR)
Duloxetine (Cymbalta)
Fluoxetine (Prozac)
Sertraline (Zoloft)

ANTI-DIARRHEAL
Diphenoxylate/Atropine
(Lonox, Lomotil)

ANTI-FUNGALS
Clotrimazole (Mycelex, Lotrimin)
Fluconazole (Diflucan)
Itraconazole (Sporonox)
Ketoconazole (Nizoral)
Voriconazole (Vfend)

ANTI -PSYCHOTIC
Olanzapine (Zyprexa)

ANTI-VIRALS
Acyclovir (Zovirax)
Cidofovir (Vistide)
Valacyclovir (Valtrex)
Valganciclovir (Valcyte)

HEPATITIS
Adelfovir (Hepsera)
Peg Interferon Alfa-2a (Peyasys)
Pegylated Intrerferon (Peg-Intron)
Ribavirin (Rebetron)

HYPOGLYCEMICS
Glipizide (Glucotrol)
Metformin (Glucophage)

LIPID LOWERING AGENTS
Atorvastatin (Lipitor)

PCP PROPHYLAXIS
Aerosolized Pentamidine (NebuPent)
Atovaquone Suspension (Mepron)
Dapsone
Sulfamethoxazole/Trimethoprim
(Bactrim)

TOPICAL STEROIDS
Hydrocortisone Cream 1%
Hydrocortisone Cream 2.5%

TOPICAL ANESTHETICS
Lidocaine (Lidoderm) Patch

WEIGHT LOSS/WASTING
Dronabinol (Marinol)**
Megestrol Acetate (Megace)
Oxandrolone (Oxandrin)**

MISCELLANEOUS
Therobec Plus (Berocca Plus)
Erythropoietin Alpha
(Epogen, Procrit)
Gabapentin (Neurontin)

**** DENOTES CONTROLLED SUBSTANCES, AVAILABLE AT ANY CARE PHARMACY**

Updated 03/24/06

64 New York Avenue, NE, Washington, DC 20002 Suite 5001 Tel (202) 671-4900 Fax (202) 673-4365

POUNDS -KILOGRAMS CONVERSION TABLE

1 POUND = 0.45359 kilogram
1 KILOGRAM = 2.2 pounds

Pounds	=	Kilograms	Pounds	=	Kilograms
1	=	0.45	100	=	45.36
5	=	2.27	105	=	47.63
10	=	4.54	110	=	49.90
15	=	6.80	115	=	52.16
20	=	9.07	120	=	54.43
25	=	11.34	125	=	56.70
30	=	13.61	130	=	58.91
35	=	15.88	135	=	61.24
40	=	18.14	140	=	63.50
45	=	20.41	145	=	65.77
50	=	22.68	150	=	68.04
55	=	24.95	155	=	70.31
60	=	27.22	160	=	72.58
65	=	29.48	165	=	74.84
70	=	31.75	170	=	77.11
75	=	34.02	175	=	79.38
80	=	36.29	180	=	81.65
85	=	38.56	185	=	83.92
90	=	40.82	190	=	86.18
95	=	43.09	195	=	88.45
			200	=	90.72

PHARMACOKINETIC FORMULAS

A. Ideal Body Weight

For dosing purposes, ideal body weight (IBW) can be estimated using the following equations:

Adults

IBWmale = 50 + (2.3 kg per inch > 5 feet)

IBWfemale = 45.5 + (2.3 kg per inch > 5 feet)

Children

$$IBW = (Height^2 \times 1.65)/1000$$

where IBW is expressed in kilograms, height in centimeters

B. Creatinine Clearance

A patient's renal function can be estimated by using the following equations:

For patients > 18 years old (Cockcroft-Gault Equation)

$$Clcr = \frac{(140 - age) \times IBW \times G}{72 \times Scr}$$

For patients 1-18 years of age

$$Clcr = \frac{0.48 \times height \times BSA}{1.73 \times Scr}$$

Where age is in years, IBW is ideal body weight in kilograms, Scr is the patient's serum creatinine in milligrams per deciliter, G is the gender factor (1.0 if male and 0.85 if female), height is in centimeters, and BSA is body surface area in square meters. The use of the patient's ideal body weight (IBW) is recommended for the Cockcroft-Gault equation. If the patient's actual body weight is less than ideal, actual weight should be used in the calculation. Daily creatinine production is approximately 15% less in females than males; therefore creatinine clearance estimates should be adjusted for gender. The normal creatinine clearance for females is 100mL/min and 125 mL/min for males. Calculated creatinine clearance provides an acceptable estimate of the patient's renal function except when the patient:

- is younger than 25 years of age or older than 90 years of age
- is undergoing dialysis
- is uremic (Scr>8 mg/dL)
- is markedly emaciated or morbidly obese
- has a rapidly changing (either up or down) serum creatinine

Elderly patients generally have less muscle mass resulting in decreased endogenous creatinine production. Utilizing the serum creatinine in these patients to estimate creatinine clearance may overestimate renal function. In emaciated patients, although their actual creatinine clearance is less than calculated (because of decreased creatinine production), it is not possible to predict easily how much less. In patients with rapidly rising serum creatinines (i.e., >0.5-0.7mg/dL/d) it is best to assume that the patient's creatinine clearance is <10mL/min.

The estimated creatinine clearance is used clinically to guide dosage adjustments for renally eliminated drugs.

C. Creatinine Clearance Values in Renal Dysfunction

Renal Function	Clcr (ML/min)
Normal	>80
Mild impairment	50-80
Moderate impairment	30-50
Severe impairment	10-30
Marked impairment	<10

D. BODY SURFACE AREA (square meters)

$$BSA = 0.007184 \times (\text{height in cm})^{0.725} \times (\text{weight in kg})^{0.425}$$

TEMPERATURE CONVERSION:

Centigrade to Fahrenheit: F = 32 + 9/5 x C

Fahrenheit to Centigrade: C = 5/9 x (F -32)

Glucocorticoid Equivalencies, Potencies, and Half-Life

Glucocorticoid	Equivalent potency dose (mg)[1]	Anti-inflammatory potency[1]	Sodium-retaining potency	Half-life plasma (min)
Short-acting				
Cortisone	25	0.8	2	30
Hydrocortisone	20	1	2	80-118
Intermediate-acting				
Prednisone	5	4	1	60
Prednisolone	5	4	1	115-212
Triamcinolone	4	5	0	200+
Methylprednisolone	4	5	0	78-188
Long-acting				
Dexamethasone	0.75	20-30	0	110-210
Betamethasone	0.6-0.75	20-30	0	300+

[1] When converting doses, use only equivalent potency column, not anti-inflammatory potency column.

Reference:

"Adrenocortical Steroids", Facts and Comparison, 2005, pg 321.

Approximate Dosage Equivalents of Thyroid Products[1]

Preparation	Composition Ratio T_4	Composition Ratio T_3	Dosage Equivalents
Thyroid desiccated	4	1	˜ 60 to 65 mg (1 grain)
Levothyroxine	1	0	˜ 50 to 60 mcg (range, 50 to 100 mcg)
Liothyronine	0	1	˜ 25 mcg (range, 15 to 37.5 mcg)
Liotrix	4	1	˜ 1 grain (12.5 mcg T_3/50 mcg T_4

[1] References may vary in dosage equivalent recommendations.

References: "Thyroid Drugs," Facts and Comparisons, 2005, pg 33

NARCOTIC AGONISTS

Comparative Pharmacokinetics

Drug	Oneset (min)	Peak (h)	Duration (h)	Half-Life (h)	Average Dosing Interval (h)		Equianalgesic Doses[1] (mg)	
							I.M.	Oral
Alfentanil	Immediate	ND	ND	1-2	—	—	ND	NA
Buprenorphine	15	1	4-8	2-3			0.4	—
Butorphanol	I.M.: 30-60; I.V.: 4-5	0.5-1	3-5	2.5-3.5	3	(3-6)	2	—
Codeine	P.O.: 30-60; I.M.: 10-30	0.5-1	4-6	3-4	3	(3-6)	120	200
Fentanyl	I.M.: 7-15 I.V.: Immediate	ND	1-2	1.5-6	1	(0.5-2)	0.1	NA
Hydrocodone	ND	ND	4-8	3.3-4.4	6	(4-8)	ND	ND
Hydromorphone	P.O.: 15-30	0.5-1	4-6	2-4	4	(3-6)	1.5	7.5
Levorphanol	P.O.: 10-60	0.5-1	4-8	12-16	6	(6-24)	2 (A) 1 (C)	4 (A) 1 (C)
Meperidine	P.O./I.M./Sub-Q: 10-15 I.V.: =5	0.5-1	2-4	3-4	3	(2-4)	75	300
Methadone	P.O.: 30-60; I.V.: 10-20	0.5-1	4-6 (acute); >8 (chronic)	15-30	8	(6-12)	10 (A) 2-4 (C)	20 (A) 2-4 (C)
Morphine	P.O.: 15-60 I.V.: =5	P.O./I.M./Sub-Q: 0.5-1; I.V.: 0.3	3-6	2-4	4	(3-6)	10	60[2] (A) 30 (C)
Nalbuphine	I.M.: 30; I.V.: 1-3	1	3-6	5		—	10	—
Oxycodone	P.O.: 10-15	0.5-1	4-6	3-4	4	(3-6)	NA	20
Oxymorphone	5-15	0.5-1	3-6				1	10[3]
Pentazocine	15-20	0.25-1	3-4	2-3	3	(3-6)		
Propoxyphene	P.O.: 30-60	2-2.5	4-6	3.5-15	6	(4-8)	ND	130[4]-200[5]
Remifentanil	1-3	<0.3	0.1-0.2	0.15-0.3	—	—	ND	ND
Sufentanil	1.3-3	ND	ND	2.5-3	—	—	0.02	NA

ND = no data available. NA = not applicable. (A) = acute, (C) = chronic.

[1] Based on acute, short-term use. Chronic administration may alter pharmacokinetics and decrease the oral parenteral dose ratio. The morphine oral-parenteral ratio decreases to ~1.5-2.5:1 upon chronic dosing.

[2] Extensive survey data suggest that the relative potency of I.M.:P.O. morphine of 1:6 changes to 1:2-3 with chronic dosing.

[3] Rectal

[4] HCl salt

[5] Napsylate salt

Ref.: **Drug Information Handbook,** 13th Ed. 2005-2006, pg. 1668.

GUIDELINES FOR DRUG LEVELS COMMONLY MONITORED

Drug	When to Sample	Therapeutic Levels
Antibiotics Gentamicin	30 min after infusion Trough <0.5 h before next dose	Peak 4-10 mcg/mL Trough <2.0 mcg/mL
Tobramycin		
Amikacin		Peak 20-35 mcg/mL Trough<8mcg/mL
Vancomycin	Peak 1 h after 1 h infusion Trough <0.5 h before next dose	Peak 25-40 mcg/mL Trough 5-10 mcg/mL
Anticonvulsants Carbamazepine	Trough just before next oral dose	4-12 mcg/mL
Ethosuximide	Trough just before next oral dose	40-100mcg/mL
Phenobarbital	Trough just before next dose	15-40 mcg/mL
Phenytoin (free)	Trough just before next dose	1-2 mcg/mL
Phenytoin (total)	Trough just before next dose	10-20 mcg/mL
Primidone	Trough Just before next dose (Note: Primidone is metabolized to phenobarb. Order levels separately)	5-12 mcg/mL
Valproic acid	Trough just before next dose	50-100 mcg/mL
Bronchodilators Aminophylline (I.V.)	18-24h after starting or changing a maintenance dose given as a constant infusion	10-20 mcg/mL
Theophylline (P.O)	Peak levels: Not recommended trough level. Just before next dose	10-20 mcg/mL
Cardiovascular Agents Digoxin	Trough just before next dose 8-24 hours after dose administered	0.5-2ng/mL
Lidocaine	Stead-state levels are usually achieved after 6-12h	15-5.0 mcg/mL
Procainamide	Trough just before next oral dose I.V. 6-12h after infusion started	4-10 mcg/mL NAPA 6-20 mcg/mL
Quinidine	Trough just before next oral dose	2-5 mcg/mL
Other Agents Amitriptyline Plus nortriptyline	Trough: just before next dose	80-250 ng/mL
Nortriptyline	Trough: just before next dose	50-150 ng/mL
Lithum	Trough just before next dose	0.6-1.5 mEq/mL
imipramine plus desipramine	Trough: just before next dose	150-250 ng/mL
desipramine	Trough: just before next dose	125-300 ng/mL

Adjustment of Serum concentration in Patients With Low Serum Albumin

Measured Total Phenytoin Concentration (mcg/mL)	Patient' s Serum Albumin (g/dL)			
	3.5	3	2.5	2
	Adjusted Total Phenytoin Concentration (mcg/mL)*			
5	6	7	8	10
10	13	14	17	20
15	19	21	25	30

*Adjusted concentration = measured total concentration ÷ [(0.2 x albumin) + 0.1]

Ref. Drug Information Handbook 13th Ed. 2005-2006 pg 1199

DRUGS WHICH MAY CAUSE DISCOLORATION OF THE FECES:

Therapeutic Category	**Color Imparted To the Feces**	**Drug(s) Responsible**
Analgesiscs (CNS)	Pink to red to black (Resulting from internal Bleeding)	salicylates
Analgesics (urinary)	Orange-red	Phenazopyridine (Pyridium)
Antacids	Whitish discoloration or speckling of feces	e.g., aluminum hydroxide preparations
Anthelminthics	Blue Red	dithiazinine (Delvex) pyrvinium pamoate (Povan)
Antibacterial agents	Black	bismuth sodium triglycollamate (Bistrimate)
Anticoagulants	Pink to red to black (Resulting from internal bleeding)	All anti- coagulants
Antiprotozoal agents	Black	bismuth glycoly- larsanilate (Milibis)
Hermatinic agents	Black	iron preparations (e.g. ferrous sulfate)
Laxatives, cathartics	Can lead to a brownish staining of the rectal mucosa	1, 8-dihydroxyanthraquinone (Dorbane; Doxan)

DRUGS WHICH MAY CAUSE DISCOLORATION OF THE URINE:

Therapeutic Category	Color Imparted To the Urine	Drug(s) Responsible
Analgesics (urinary)	Orange to orange-red	ethoxazene (Serenium) phenazopyridine (Pyridium)
Antibacterial agents	Orange-yellow (in alkaline urine)	salicylazosulfapyridine (Azulfidine)
	Discoloration (No specific effect)	p-aminosalicylic acid and derivatives
	Rust yellow or brownish	sulfonamides nitrofurantoin and derivatives, e.g. furazolidone (Furoxone)
Anticoagulants	Orange (in alkaline urine), pink or red to red-brown	indanedione derivatives (e.g. anisindione (Hedulin)
Anticonvulsants	Pink or red to red-brown	diphenylhydantoin (Dilantin) phensuximide (Milontin)
Antidepressants	Blue-green	amitriptyline (Elavil)
Antidote to cyanide poisoning	Blue or green	methylene blue
Antiprotozoal agents	Brown to black	quinine and derivatives
	Rust yellow or brown	pamaquine naphthoate (Plasmochin) primaquine chloroquine (Aralen)
	Yellow	quinacrine (Atabrine)
	Dark	metronidazole (Flagyl)
Diuretics	Pale blue Fluorescence	triamterene (Dyrenium)
Hemostatic agents	Blue-green	tolonium (Blutene)
Hematinic agents	Black	iron-sorbitolcitric acid complex (Jectofer)
Laxatives, cathartics	Brown to black	cascara; rhubarb
	Pink to red or red-brown	1,8- dihydroxyanthraquinone emodin (in alkaline urine) phenolphthalein
Skeletal muscle relaxants	Orange or purplish-red	chlorzaxazone (Paraflex)
	Dark, brown to black or green on standing	methocarbamol (Robaxin)
Tranquilizers	Pink to red or red-brown	Phenothiazines
Vitamins	Yellow	riboflavin

DRUGS WHICH AFFECT LABORATORY VALUES

Drugs can and do influence laboratory diagnostic tests. Those involved in patient care must be aware of these effects and the misleading results they cause.

The following chart lists some of the drugs and procedures which are known to affect laboratory determinations. The chart is not intended to represent a complete listing of such effects, but to serve as a guide.

TEST	DRUG	EFFECT
Urine: Acetone	Sulfobromophthalein (BROMSULPHALEIN), Phenolsulfonphthalein	Increase value
Kidney Function	Sulfobromophthalein-(BROMSULPHALEIN)	Interferes with reading of phenolsulfonphtalein test (24 hours required between drugs)
Urine: Diacetic acid	Phenothiazines & Salicylates	Increases values
Urine: Albumin	Penicillin (massive doses), Salicylates, Tolbutamide, X-Ray contrast media	Increases albumin excretion causing false positive
Urine: Amino Acids	Cortropin (Acth), Cortisone, Sulfonamides	Increase excretion of Amino acids
	Epinephrine, Insulin	Decrease excretion of amino acids
Urine: Catecholamines	Erythromycin, Methyldopa (ALDOMET), Quinidine, Tetracyclines, Hypertensive agents, B-complex vitamins Epinephrine-like agents used in asthma	Increse catecholamine content
Blood: Enzymes		
Acid Phosphatase	Androgens, Prostate Massage	Increase blood level
Alkaline Phasphatase	Methyldopa (ALDOMET)	Variable effect
Serum Amylase	Morphine, Codeine, Meperidine (DEMEROL)	Increase level up to 24 hours
	Alcohol	Increase level
SGOT	Opiates, Salicylates Methicillin, Ampicillin	Increase level
	Methyldopa	Variable effect

DRUGS WHICH AFFECT LABORATORY VALUES (Cont' d.)

TEST	DRUG	EFFECT
Liver Function	Anabolic steroids, Barbiturates Estrogens, Morphine, Probenecid, Phenazopyridine (PYRIDUM) Iopanoic Acid (TELAPAQUE)	Increase retention of Sulfobromophtalein
Serum Bilirubin	Caffeine Methyldopa	Decrease level Variable effect
Blood Ammonia	Sodium salts	may cause increase
	Ion exchange (e.g. KAYEXALATE)	may cause increase
Prothrombin	Barbiturates	Increase prothrombin activity
	Antibiotics, Globulin, Salicylates, sulfonamides, Hydroxyzine (VISTARIL)	Decrease prothrombin activity
	Methyldopa	Variable effect
Serum Albumin	Penicillin (massive doses), Salicylates, Tolbutamide, X-ray contrast media	Increase values
Blood Urea Nitrogen	Chloral Hydrate, Triamterene (DYRINIUM) Methyldopa	Increase BUN
	Glucose infusion	Decrease BUN
Serum Proteins	Sulfobromophthalein	Elevated value
	Ammonium salts	Decrease value
Serum Calcium	Heparin, Insulin	May decrease levels
Serum Sodium	Calcium salts, Potassium salts, Seroids	May increase levels
	Diuretics, paracentesis	May decrease levels
Serum Potassium	Hyperventilation, Cortropin (ACTH), steroids, Sulfates and Phosphates	Decrease levels
Serum Phosphorous	Epinephrine, Insulin, general anesthetics	Decrease levels
Serum Chloride	Acetazolamide (DIAMOX), Bromides, Ion exchange resins, steroids	Increase values
	Cortropin (ACTH), diuretics	Decrease levels
Serum Copper	Iron and Cobalt preparations	Increase values
Serum Iron and Iron Binding Capacity	Cortropin (ACTH) and steroids	Decrease values
	Iron-Dextran Complex (IMFERON)	Increase values

DRUGS WHICH AFFECT LABORATORY VALUES (cont' d.)

TEST	DRUG	EFFECT
Blood Cholesterol	Cortropin (ACTH), Cortisone, Vitamin A, Bromides	Usually raise level
	Androgens, Thyroid, Heparin, Clofibrate (ATROMID-S)	Decrease level
Blood Glucose	Oral Contraceptives	Decrease glucose Tolerance curve
	Cortropin (ACTH)	Increase level
Protein-Bound Iodine	X-ray contrast media	Increases values for as long as 10 years
	Barium Sulfate, Oral Contraceptives, Estrogens, Amebacides (e.g. FLORAQUIN, VIOFORM), Suntan Oil, Mouthwashes, Vitamin preparations, Iodized salt	Increase values
	Liothyronine (CYTOMEL), Testosterone, Cortropin (ACTH), Chlorates, Cortisone, Mercurial Diuretics, Salicylates, Sulfonamides	Decrease values
	Sulfobromophthalein	Variable effect
Uric Acid	Dicumarol, Piperazine (ANTEPAR), Cortropin (ACTH)	Decrease values
	Nitrogen Mustard (MUSTARGEN), Chlorothiazide (DIURIL), Pyrazinamide	Increase values
	Methyldopa	Variable effects
Creatinine	Ascorbic Acid, Sulfobromophthalein, Phenolsulfonphthalein	Increase level
Blood Cross Match: Direct Coombs Test	Methyldopa (ALDOMET) Cephalothin (KEFLIN) Penicillin	False positive (up to one year)

District of Columbia Health Care Alliance
Request For Formulary Change

PHYSICIAN: _____,MD DATE: _____

ADDRESS: _____ PHONE#: _____

_____ FAX#: _____

INSTRUCTIONS: Requesting physician must complete "A" thru "H" in full.
The completed form should be forwarded to: Department of Health Warehouse, #4 D.C. Village Lane S.W., Washington D.C. 20032 Fax: 202 645-6263

A. Name of Drug: _____ B. Manufacturer:_____
C. Dosage Form Desired: Tablet ( ) Capsule ( ) Ointment ( )
Ampule ( ) Liquid ( ) Powder ( )
Other (Specify) _____
D. Dosage Strength(s) Desired: _____
E. Technical Information:

1. Indication(s) _____
_____
_____
2. Action(s) _____
_____
_____
3. Uses: _____
_____
_____
4. Contraindications: _____
_____
_____
5. Adverse Reactions – Frequency and Intensity: _____
_____
_____

F. Is there a Similar-Acting Drug now carried on formulary? Yes____ No____
G. Formulary Drug it may replace: _____
_____
H. What are the advantages of the drug requested over the one now stocked? _____
_____
_____

Action of the Pharmacy and Therapeutics Committee:

Accepted ( ); Rejected ( ); Other ( ) – Explain _____

Remarks: _____

Date: _____ _____
Chairman

District of Columbia
Department of Health
Medical Assistance Administration
Office of Managed Care

Continuous Quality Improvement Plan For Oversight and Assessment of Medicaid Managed Care Organizations

March 18, 2004

Table of Contents

I. Purpose 3

II. Scope 3

III. The District's Medicaid Managed Care Program 3

IV. Mission, Vision, Values & Guiding Principles 4

A. Mission 4
B. Vision 4
C. Values & Guiding Principles 4

V. Goals & Objectives 5

A. The District's Standards for Access to Care 5
1. Availability of Services 5
2. Assurances of Adequate Capacity and Services 7
3. Coordination and Continuity of Care 7
4. Coverage and Authorization of Services 9
B. The District's Standards for Structure and Operations 10
1. Provider Selection 10
2. Beneficiary Information 10
3. Confidentiality 10
4. Enrollment and Disenrollment 11
5. Grievance Systems 11
6. Subcontractual Relationships and Delegation 11
C. The District's Standards for Quality Measurement and Improvement 11
1. Practice Guidelines 11
2. Quality Assessment and Performance Improvement Program 12
3. Health Information Systems 12
4. Quality Measurement and Improvement Standards 13
5. Non-duplication of Mandatory Activities 15
6. State Monitoring and Evaluation 15
7. Procedure for Race, Ethnicity, and Primary Language 16
8. National Performance Measures and Levels 16
9. Intermediate Sanctions 16
D. Additional Information for Persons with Special Health Care Needs 17
1. Promote and Monitor Access to Services 17
2. Promote and Monitor Services to Special Needs Populations 18
3. Ensure Compliance with EPSDT Requirements 20
E. Additional Information related to Structure and Operations Standards 22
1. Organizational Standards 22
2. Decision Resolution Processes 24
a. Complaint Process 24
Exhibit I 25
b. Grievances and Appeals 26

VI. Conclusion 33

VII. Definitions & Acronyms 35

I. Purpose

The Department of Health, Medical Assistance Administration (MAA), Office of Managed Care (OMC) will maintain an active Continuous Quality Improvement (CQI) Plan, herein the Plan, for oversight and assessment of the District of Columbia's (District) Medicaid Managed Care Organizations[1] (MCOs) to ensure that individuals receiving care and services under the District of Columbia Healthy Families Program (DCHFP) have access to appropriate, essential, quality and cost effective health care services.

II. Scope

The Plan will outline and briefly describe the quality monitoring and oversight strategies of the District's MCOs for the provision of care to Medicaid MCOs' beneficiaries. This Plan will also focus on the performance of important functions that significantly affect the health outcomes and perceptions of Medicaid MCOs' beneficiaries regarding the quality, safety, and value of services provided. These functions include collecting, measuring, and analyzing information, as well as evaluating, and monitoring services rendered to beneficiaries. In addition, these functions impact beneficiary satisfaction and also measure the administrative capacity of MCOs. The information will then be used to: (1) identify high quality performance, (2) assess quality improvement, (3) foster collaboration and communication between MAA and MCOs, and (4) manage the District's Medicaid managed care program.

III. The District's Medicaid Managed Care Program

The Government of the District of Columbia, Department of Health, Medical Assistance Administration is the single state agency with the responsibility for implementation and administration of the District's Medicaid and State Children's Health Insurance Programs (SCHIP). Since April 1994, the District operated a Medicaid managed care program for its Temporary Assistance to Needy Families (TANF) population through the MAA. Since 1996, the District operated a Medicaid demonstration project that provided services for Social Security Insurance (SSI) or SSI-eligible children through a managed care organization. In 1998, the District extended health insurance coverage to children in families earning up to 200 percent of the Federal Poverty Level (FPL) through a combined Medicaid and State Children's Health Insurance Program. Approximately 65 percent of Medicaid beneficiaries in the District participated in managed care and received care through one of seven MCOs.

In October 2002, there was a reduction in the number of MCOs serving DC Medicaid beneficiaries from seven to four. The average monthly census for the District's remaining four MCOs was 85,254 beneficiaries. Of these 85,254 beneficiaries, approximately 57,023 were eligible children, including 2,636 that were eligible for SCHIP, and 25,595 that were adults eligible for SCHIP. Approximately 2,600 SSI children were enrolled in a special provider MCO for children. In late 2002, the District's goal was to extend Medicaid coverage to a maximum of 2,400 childless adults ages 50 to 64.

---

[1] For the purpose of this document, and where appropriate, the term MCO may also include a Prepaid Inpatient Health Plan or PIHP, and/or the Child and Adolescent Supplemental Security Income Program or CASSIP.)

The implementation and management of the District's Medicaid Managed Care Program continues to be successful. It is transitioning from a start-up project to a mature program that is redesigning its processes, policies, procedures, operations, and organizations to perform effectively as it moves toward a more enhanced phase of growth and development. This Plan is a part of that redesigning effort.

IV. Mission, Vision, Values & Guiding Principles

A. Mission

The mission of the Office of Managed Care is to lead and manage MCOs by utilizing the District's resources to promote and improve the health status and well-being of low-income families, indigent individuals, and families with special health care needs who receive health services through the District's Medicaid Managed Care Program.

The Office of Managed Care fulfills its mission through planning, setting policies and requirements, pursuing resources, developing programs, providing program oversight, and ensuring fiscal accountability to promote an accessible system of quality care for the District's Medicaid managed care population.

B. Vision

The vision of the Office of Managed Care is to ensure accessible and appropriate quality health care services for all of the District's Medicaid managed care beneficiaries.

C. Values & Guiding Principles

- Access – Ensure and support efforts to remove any barriers to health care services and resources, including but not limited to language barriers.
- Quality – Commit to program excellence and continuous quality improvement.
- Beneficiary Satisfaction – Listen to, understand, and address the needs of beneficiaries and stakeholders in a prompt, respectful, and responsive manner.
- Cultural and Linguistic Competence – Provide appropriate services that are responsive and accessible to a diverse population.
- Accountability – Demonstrate responsibility to stakeholders.
- Integrity – Perform responsibilities with honesty, sincerity, courtesy and the highest quality of ethical and professional conduct.
- Communication – Promote an open exchange of information and ideas with a commitment to listen and respond accurately, reliably, and in a timely manner to beneficiaries and stakeholders.

- Commitment – Remain faithful and dedicated to the mission and vision of the program.

V. Goals & Objectives of the District's Medicaid Managed Care Program

The goals of the managed care program are to purchase the best value health care for MAA beneficiaries, to improve access to services for underserved and vulnerable beneficiary populations, and to protect them from substandard care. This Plan will detail several objectives to assess, monitor, and measure the improvement in health care services provided to Medicaid managed care beneficiaries within the District of Columbia by the contracted Managed Care Organizations.

A. District of Columbia Standards for Access to Care are at least as stringent as those specified in 42 CFR 438.206-438.210.

- Availability of Services
- Assurances of Adequate Capacity and Services
- Coordination and Continuity of Care
- Coverage and Authorization of Services
- Provider Selection
- Beneficiary Information
- Confidentiality
- Enrollment and Disenrollment
- Grievance Systems
- Subcontractual Relationships and Delegation
- Practice Guidelines
- Quality Assessment and Performance Improvement Program
- Health Information Systems
- Quality Measurements and Improvement Standards
- State Monitoring and Evaluation Activity
- Procedures for Race, Ethnicity, and Primary Language
- National Performance Measures and Levels
- Intermediate Sanctions

1. Availability of Services

a. *Maintains a Network of Appropriate Providers*
Enrollment counselors have access to up-to-date information about the provider network for each MCO. This information is critical in assisting beneficiaries in selecting a health plan that will ensure continuity of care for persons receiving services at the time of enrollment. The data include primary care providers (PCP), hospitals, clinics, pharmacies, and specialists. A major emphasis focuses on assisting beneficiaries who are receiving care during enrollment, to select a health plan that will enable them to continue their current provider relationship. MAA monitors the provider network to assure that there will be providers within the standards for distance and travel time. Each MCO will regularly submit provider listings to MAA in order to demonstrate that the plan has a provider network that is able to provide the covered services in accordance with the terms and conditions of the contract.

b. *Provides Beneficiaries with Direct Access to a Women's Health Specialist:* In accordance with terms and conditions of the contract, MCOs must provide female beneficiaries with direct access to a women's health specialist within a provider network for covered care necessary to provide routine medical, maternity, and preventive health care services in addition to the beneficiary's designated PCP. If the PCP is not a women's health specialist, the MCO must allow female beneficiaries to self refer to either an in-network or non-network women's health specialist.

c. *Provides for a Second Opinion from a Qualified Health Professional:* In addition to providing for a second opinion from a qualified health care professional within the network, the MCO shall arrange for the beneficiary to obtain one (1) second opinion outside the network, at no cost to the beneficiary, as specified in 42 CFR 438.206 (b)(c).

d. *Provides Services Not Available In-Network:* If the network is unable to provide necessary services covered under the MCO contract to a particular beneficiary, the MCO must adequately and timely cover these services out-of-network for the beneficiary, for as long as the MCO is unable to provide the coverage. This also includes family planning services.

e. *Coordination of Payment with Out-of-Network Providers:* MCOs must coordinate with out-of-network providers with respect to payments and ensure that the cost to the beneficiary is no greater than it would be if services were rendered in-network.

f. *Demonstrates Providers are Credentialed:* MCOs must have a credentialing and re-credentialing process for physicians and other licensed health care professionals including member physician groups. This is based on a written application and site visits as appropriate, and at a minimum, primary source verification of licensure, education, training, experience, privilege(s), disciplinary status, and eligibility for payment under Medicaid. This process ensures that physicians and other licensed health care professionals are and will remain in compliance with any Federal and District of Columbia requirements.

g. *Timely Access to Services:* Under contractual terms and conditions, MCOs must ensure and require that their providers meet District standards for timely access to care and services while taking into account the urgency of the need for services. MCOs must also regularly monitor providers, including mental health and substance abuse providers, to assure compliance with timely access standards and when necessary, take corrective action for failures to comply. In accordance with 42 CFR 438.206 (c) (ii) and 438.207, MCOs must ensure that network providers offer hours of operation that are no less than the hours of operation offered to commercial beneficiaries or comparable to Medicaid fee-for-service, if the provider serves only Medicaid beneficiaries.

h. *Cultural Considerations:* In accordance with 42 CFR 438.206 (c)(2), cultural competency training must be required for clinical and non-clinical MCO staff members who interact on a regular basis with beneficiaries. This includes but is not limited to member services, scheduling, billing, transportation, and appeal, and grievance staff. MCOs must ensure that services are provided in a cultural competency manner to all beneficiaries. MCOs are required to participate in MAA's efforts to promote the delivery of services in a cultural competency manner. In addition, all beneficiary materials must meet cultural competency requirements, as well as reading level and language needs.

2. Assurances of Adequate Capacity and Services

a. *Offers an Appropriate Range of Preventive, Primary Care and Specialty Services:* Under the terms and conditions of the contract, MCOs must maintain an adequate and accurate network of health service providers. They include primary care providers, hospitals, clinics, pharmacies, and specialists that (i) are of sufficient size and scope to meet the health needs of the beneficiaries; (ii) provide the items and services included under covered benefits; and (iii) provide the mental health and alcohol and drug abuse care needs of the Medicaid beneficiaries.

b. *Maintains a Network of Providers that is Sufficient in Number, Mix, and Geographical Distribution*: Each MCO is required to demonstrate adequate capacity in order to begin enrollment for beneficiaries. Each MCO is responsible for regularly submitting provider listings including languages spoken by providers to demonstrate that the plan has a provider network that is able to ensure that the services are covered in accordance with the terms and conditions of the contract. The network must include PCPs in sufficient numbers so that no PCP has more than two thousand (2,000) Medicaid beneficiaries. MCOs must also assure that the geographical location of providers and Medicaid beneficiaries, and must consider distance, travel time, and means of transportation ordinarily used by Medicaid beneficiaries, and whether the location provides physical access for Medicaid beneficiaries with disabilities. All beneficiaries will have the option to select between at least two PCPs located within thirty (30) minutes of their place of residence utilizing public transportation. MAA will monitor provider and service capacity quarterly. In addition to monitoring the number of providers available by specialty and type in each MCO, MAA will review the number of PCPs, dentists, and mental health practitioners with closed panels, partially closed panels, and open panels.

3. Coordination and Continuity of Care

a. *Ensure that Each Beneficiary has an Ongoing Source of Primary Care*: MCOs must ensure that each beneficiary has an ongoing source of primary care appropriate to his or her needs and has a person or entity formally designated as primarily responsible for coordinating the health care services rendered to the beneficiary.

In accordance with 42 CFR 438.208, an MCO must implement procedures to deliver primary care and coordinate health care for all beneficiaries. MAA looks for three elements to determine if the MCO has a basic system in existence: (1) beneficiaries with special health care needs must receive case management services according to established criteria and must receive the appropriate care; (2) the MCO must have policies and procedures to coordinate care with other appropriate agencies or institutions; and (3) the MCO must monitor continuity of care across all services and treatment modalities.

b. *Coordinate All Services that the Beneficiaries Receives:* In accordance with 42 CFR 438.208 (c) (2-4), MCOs must maintain a care management system. This includes utilization management and care coordination that ensures all beneficiaries are regularly examined to identify potential or actual health problems requiring prevention, treatment, rehabilitation, and/or education in self-care standards for the provision of health care to adults.

c. *Share the Results of Identification and Assessment Information to Prevent Duplication of the Activities for Individuals with Special Health Care Needs*: MCOs must implement mechanisms to assess any Medicaid beneficiary identified by the District (or by the MCO) as having a special health care need. This system must operate in accordance with applicable standards for high quality provision of services, including Early and Periodic Screening, Diagnosis and Treatment (EPSDT), and Individuals with Disabilities Act (IDEA) standards to identify any ongoing special conditions of the beneficiary that require a course of treatment or regular care monitoring. The assessment mechanisms must use appropriate health care professionals. MCOs must establish procedures to ensure that medical and adjunct care is comprehensively planned with the involvement of the beneficiary, their family, or caretaker, and appropriately qualified practitioners. The beneficiary must be assisted with the coordination of services when needed, and health care resources must be used efficiently. The treatment plan must be developed by the beneficiary's PCP with beneficiary participation, and in consultation with any specialists caring for the beneficiary. MCOs must review the plan of treatment in a timely manner. However, if an MCO fails to review the plan of treatment within thirty (30) days, the plan of treatment may be implemented in accordance with any applicable District quality improvement and utilization review standards.

d. Protect the Beneficiaries' Privacy in the Process of Coordinating Care: Health plans must ensure that all individually identifiable

information relating to Medicaid beneficiaries is kept confidential pursuant to the District of Columbia regulations, 42 U.S.C. Section 1396a(a)(7) (Section 1902(a)(7) of the Federal Social Security Act), 42 CFR Part 2 and other regulations promulgated thereunder. The MCO must ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191, August 21, 1996) and all applicable regulations promulgated thereunder. Such regulations include, but are not limited to, the Medical Privacy Rule, 65 Federal Regulations 82462 (December 28, 2000) (codified at 45 C.F.R. Parts 160-164) and the electronic transactions and code set standards rule, 65 Federal Regulations 50312 (August 17, 2000) (codified at 45 C.F.R. Parts 160 and 162). MCOs must maintain written procedures for compliance with all applicable privacy, confidentiality, and information security requirements. Additionally, MCOs must train their employees and subcontractors to be in compliance with all matters applicable to privacy, confidentiality, and information security requirements.

e. *Additional Services to Persons with Special Health Care Needs:* In accordance with 42 CFR 438.208 for beneficiaries with special health care needs who have been assessed by appropriate health care professionals (consistent with 42 CFR 438.208(c)(2)) and need a course of treatment or regular care monitoring, an MCO must have a mechanism to allow beneficiaries to directly access a specialist as appropriate for the beneficiary's condition and identified needs. An MCO must ensure that the plan of treatment for a beneficiary with special health care needs will be reviewed and updated, no less frequently than every twelve (12) months or as determined by the beneficiary's PCP. MAA requires MCOs to provide care coordination/case management services for individuals with special health care needs. Each MCO must have a care coordination department directed by a senior manager with a registered nurse (RN), medical doctor (MD) or the equivalent, and must be staffed by care coordinators with appropriate clinical/medical training and experience. Care coordination must be made available to persons with special needs. The care coordinator is responsible for facilitating the development of a multidisciplinary treatment plan; providing relevant information or participating in the development of the Individualized Education Plan (IEP) or Individualized Family Services Plan (IFSP); assisting in the coordination of the treatment plan (including transfer of information); and supporting the coordination of network and non-network services. The care coordinator is also responsible for coordinating service among District Agency providers, monitoring the treatment plan, and providing periodic reassessments.

4. Coverage and Authorization of Services

a. *Identify, Define, and Specify the Amount, Duration and Scope of Each Service that the MCO is Required to Offer:* In accordance with 42 CFR

438.210, MCOs are required to furnish the identified services in an amount, duration, and scope that is no less than the amount, duration, and scope for the same services furnished to beneficiaries enrolled in the Medicaid fee-for-service program. MCOs will ensure that the services are sufficient in amount, duration, or scope to reasonably be expected to achieve the purpose for which the services are furnished. MCOs must not arbitrarily deny or reduce the amount, duration, or scope of a required service solely because of diagnosis, type of illness, or condition of the beneficiary. MCOs must place appropriate limits on a service criteria applied under the District plan, such as medical necessity, or for the purposes of utilization control, provided it is reasonably expected to achieve its prescribed purpose.

b. Specify *What Constitutes "Medically Necessary Services":* These are services in the District's Medicaid programs which meet medical necessity criteria as established in the MCO contract. The criteria include clinical determinations to establish a service or benefit that will, or is reasonably expected to, prevent the onset of an illness, condition, or disability; reduce, maintain, or ameliorate the physical, mental, behavioral, or developmental effects of an illness, condition, injury or disability; and/or assist the individual to achieve or maintain and regain maximum functional capacity in performing daily activities, taking into account the functional capacity for individuals of the same age.

c. *Written Policies and Procedures for Authorization of Services: When* processing requests for initial and continuing authorizations of services, the MCO and its subcontractors must adhere to established written policies and procedures and implement mechanisms to ensure consistent application of review criteria for authorization decisions, while consulting with the requesting provider when appropriate.

d. *Decisions to Deny Services:* In accordance with 42 CFR 438.210 (b)(3), any decision to deny a service authorization request or to authorize a service in an amount, duration, or scope that is less than requested must be made by a health care professional who has appropriate clinical experience in treating the beneficiary's condition or disease.

B. District Standards for Structure and Operations are at least as stringent as those specified in 42 CFR sections 438.214-438.230.

1. Provider Selection

In accordance with 42 CFR 438-214, MCOs must follow a uniformed credentialing and recredentialing policy as established by the District of Columbia, as well as comply with all terms, conditions and Federal regulations contained within the MCO contract related to provider selection. In developing a network of providers, MCOs must recruit, credential, evaluate, and monitor selected providers with an appropriate combination of skills, experience, and specialties to constitute a network to provide covered benefits to beneficiaries

within the acceptable geographic access standards. The MCO's provider selection policies and procedures must not discriminate against particular providers that serve high-risk populations or specialize in conditions that require costly treatment. Additionally, MCOs must not employ or contract with providers excluded from participation in Federal health care programs under either Section 1128 or Section 1128A of the Social Security Act.

2. Beneficiary Information

When reviewing medical records and any other health and enrollment information that contain identifying beneficiary information, the MCO must use and disclose information in accordance with the privacy requirements in 45 CFR parts 160 and 164, Subparts A and E, to the extent that these requirements are applicable. Such information must be used by the plan or its providers only for a purpose directly connected with performance of the plan's obligations under the Medicaid managed care program.

3. Confidentiality

MCOs must ensure that all individually identifiable information relating to Medicaid beneficiaries is kept confidential pursuant to the District of Columbia, 42 U.S.C. §1396a(a)(7), Section 1902(a)(7) of the Federal Social Security Act), 42 CFR Part 2 and other regulations promulgated thereunder. The MCO must ensure compliance with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, August 21, 1996) and all applicable regulations promulgated thereunder. Such regulations include but are not limited to, the Medical Privacy Rule 65 Federal Regulations 82462 (December 28, 2000) (codified at 45 C.F.R. Parts 160-164) and the Electronic Transactions and Code Set Standards Rule, 65 Federal Regulations 50312 (August 17, 2000) (codified at 45 C.F.R. Parts 160 and 162). MCOs must also maintain written procedures for compliance with all applicable privacy, confidentiality, and information security requirements. In addition, MCOs must train employees and subcontractors on compliance with all applicable privacy, confidentiality, and information security requirements. MCOs must provide documentation verifying that employees and subcontractors have received confidentiality, privacy, and information security training.

4. Enrollment and Disenrollment

Within the terms and conditions of the contract and according to all applicable Federal regulations, the MCO will accept each individual who is enrolled or assigned to the MCO by the District or its agents. Similarly, the MCO must abide by the terms and conditions under the contract and according to all applicable regulations related to disenrollment of a participating beneficiary.

5. Grievance Systems

The MCO must document all communications with beneficiaries, written and verbal, and must maintain written policies and procedures for the receipt and prompt resolution of complaints and grievances. These reports and documentation are subject to review by the District as deemed necessary. The

complaint and grievance system must comply with applicable Federal requirements, statutory requirements under the Social Security Act, and the District of Columbia's Office of Administrative Hearing.

6. Subcontractual Relationships and Delegation

The MCO must ensure that all activities carried out by any subcontractor conform to the provisions of the contract. The terms of any subcontracts involving the provisions or administration of medical services must be subject to MAA approval via the Contracting Officer. In accordance with 42 CFR 438.230, the District will ensure, through its contracts, that each MCO: (1) oversees and is accountable for any functions and responsibilities that it delegates to any subcontractor; and (2) meets applicable provisions related to subcontractors under the MCO contract.

C. District Standards for Quality Measurements and Improvement are as at least stringent as those specified in 42 CR 438.236-438.242

1. Practice Guidelines

In accordance with 42 CFR 438.236, the MCO must adopt practice guidelines that meet the following requirements:

a. Based on valid and reliable clinical evidence or a consensus of health care professionals in the particular field;
b. Considered the needs of the contractor's beneficiaries;
c. Adopted in consultation with contracting health care professionals; and
d. Reviewed and updated periodically, as appropriate.

MCOs must disseminate the guidelines to all affected providers and, upon request, to beneficiaries and potential beneficiaries, along with decisions for utilization management, beneficiary education, coverage of services, and other areas.

2. Quality Assessment and Performance Improvement Program

The MCO must operate and provide a description of its Continuous Quality Improvement (CQI) Program to the District for approval. MCOs must develop a written CQI Plan annually that details the plans, tasks, initiatives, and staff responsible for improving quality and meeting the requirements and beneficiary services incorporated under the MCO contract. In addition to complying with contractual terms related to specific CQI activities, processes and reporting, an MCO must have procedures that: (1) assess the quality and appropriateness of care and services furnished to all Medicaid beneficiaries and to individuals with special health care needs; (2) identify the race, ethnicity, and primary language spoken of each Medicaid beneficiary; (3) regularly monitor and evaluate an MCO's compliance with the standards for MCOs, PIHPs; and (4) comply with any national performance measures and levels that may be identified and developed by the Center for Medicare and Medicaid Services (CMS) in consultation with states and

other relevant stakeholders. Performance measures and outcome data are reported by MCOs to the MAA according to the terms of the contract.

3. Health Information Systems

In accordance with 42 CFR 438.242, the MCO must operate a Management Information System (MIS) capable of maintaining, providing, and documenting information. The MIS shall be capable of collecting, analyzing, integrating, and reporting data sufficient to document MCOs' compliance with the contract that must include but not limited to the following requirements:

a. Beneficiary eligibility data — current and historical;
b. Encounter and claim payment records — current and historical;
c. Authorization and care coordination data;
d. Utilization management;
e. Provider network information, i.e., provider affiliations, credentialing, recredentialing information;
f. EPSDT tracking;
g. Outcome reports;
h. Financial accounting data;
i. Grievance and appeals statistics;
j. Internal operations data, e.g., telephone response time;
k. Clinical information;
l. Serious incidents;
m. Beneficiary satisfaction;
n. Provider profiling;
o. Outcome measurements;
p. Disenrollment for other than loss of Medicaid eligibility; and
q. Different languages spoken by providers.

MCOs must have a MIS capable of documenting administrative and clinical procedures while maintaining confidentiality of individual medical information, including special confidentiality provisions related to people with HIV/AIDS, special health care needs, mental illness, and alcohol and drug abuse disorders. The MIS shall be capable of collecting data on beneficiary and provider characteristics as specified by the District and on services rendered through an encounter data system or other methods as specified. The encounter data reporting system should be designed to assure aggregated, unduplicated service counts provided across service categories, provider types, and treatment facilities. MCOs must have internal procedures to ensure that data reported to the District are valid and must test the validity and consistency on a regular basis. MCOs will ensure accurate and complete data, as well as verify the accuracy and timeliness of reported data; screen the data for completeness, logic, and consistency; and collect service information in standardized formats to the extent feasible and appropriate.

4. Quality Measurement and Performance Improvement

Under the District's Medicaid Managed Care Program, the MCO is the organization responsible for delivering a set of services for its beneficiaries. The District, in turn, has an obligation to monitor and assess the performance of individual MCOs as an organization and their plans for continuous performance improvement. MCOs' internal quality assessment and continuous quality improvement programs (QA/CQI) are mechanisms MCOs will use to monitor, evaluate, and improve the care delivered to beneficiaries. How each MCO implements its internal QA/CQI program is of foremost importance to MAA.

Under a risk-based contract, the MCO is required by Federal law to operate a QA/CQI program and under External Quality Review Organizations (EQRO) standards, MCOs are required to implement a QA/CQI program. MCOs' administrative functions drive the organizations to continual improvement. These functions must comply with the Quality Improvement System for Managed Care Interim Standards and Guidelines (QISMC), as well as Health Plan Employer Data and Information Set (HEDIS) or HEDIS-like measures. MCOs are expected to provide documentation that they have or are actively implementing an internal QA/CQI program that meets contract standards. In addition, MCOs are also expected to have a plan for incorporating the experience of MCOs' staff, the District, and other stakeholders into the evaluation of their QA/CQI program.

The District oversees, monitors, and evaluates MCOs on a host of activities related to quality assessment and continuous quality improvement. This oversight allows MAA to evaluate the quality and appropriateness of the care and services rendered to all Medicaid beneficiaries, and to ensure compliance with contract provisions. Specific examples of review related to quality include:

a. Special Performance Improvement Projects;
b. Performance Measurement Data; Care Coordination (PCP, MCOs' provider and care contractors);
c. Special Health Care Needs (children and adults)
    i. Identification
    ii. Assessment
    iii. Case Management
d. Clinical Performance Measures and Standards
e. Beneficiary Satisfaction Surveys;
f. Utilization Management Criteria (case management);
g. Complaints, Grievance, and Administrative Hearing (clinical care); and
h. Clinical Quality of Case Studies

MAA contracts with an EQRO to perform an annual review of the MCOs' QA/CQI programs. The annual review consists of an assessment of the structure, process and outcome of each MCO's internal QA/CQI program. It also includes review of records and corrective action plan(s) for continuous quality improvement.

Currently, improvement has been achieved for the majority of the MCOs. The QA/CQI process has been enhanced by an increase in human resources and

data integration capabilities. The ability to move from traditional "case" management to integrated "coordination of care" expanded the scope of the QA/CQI programs with an increased ability to measure outcomes and continually evaluate the level of care and services provided to the beneficiaries. Improvement also exists in the data collection capabilities of MCOs with integration of health/pharmacy claims, encounters, member services, medical management, provider/beneficiary satisfaction surveys, sentinel and adverse events, and credentialing reports which move from "focused" capabilities to concurrent identification of patterns for tracking and trending of their entire patient population. Clinical studies utilized evidence-based criteria, national clinical guidelines, and the ability for re-measurement of intervention effectiveness over time. These studies served as impetus for the creation of disease management programs that deliver specialized services for Asthma, Diabetes, HIV/AIDS, Hypertension, Congestive Heart Failure, Chronic Obstructive Pulmonary Disease, and high-risk maternity populations.

As part of its quality monitoring and oversight activities, MAA will continue to review and approve, at least annually, how well MCOs are implementing and revising its QA/CQI program and process, and the impact and effectiveness of the Medicaid managed care program. In addition, MAA will audit MCOs to target opportunities for QA/CQI and then work in collaboration with the EQRO and with MCOs to monitor continuous quality improvement programs. These include provisions for (1) performance on access and service issues and compliance, (2) program development, (3) monitoring, (4) problem resolution, and (5) reporting requirements. MAA will also collaborate with MCOs to proactively develop programs for the District's changing population, and to work with community health clinics and other providers in underserved areas that currently do not meet MCOs' continuous quality improvement requirements.

5. Non-duplication of Mandatory Activities

In accordance with §438.360 on non-duplication of mandatory activities, the District may use, in place of a Medicaid review by the State, its agent, or EQRO, information about the MCO obtained from a Medicare or private accreditation review to provide information otherwise obtained from the mandatory activities specified in §438.358(b) and optional activities specified in §438.358 (c). The District will identify the standards for which the EQR will use information from Medicare or private accreditation reviews, and will explain its rationale for why the standards are duplicative.

If the EQRO obtains information from a Medicare or private accrediting organizations reviewing the MCO, the MCO must be in compliance with standards established by CMS for Medicare+Choice or a national accrediting organization. The CMS or national accreditation standards must be comparable to standards established by the District to comply with §438.204(g) and the EQR-related activity under §438.358(b)(3). Compliance with the standards is determined either by: (1) CMS or its contractor for Medicare, or (2) a private national accrediting organization that CMS has approved as applying standards at least as stringent as Medicare under the procedures in §422.158. The MCO must provide to the District all the reports, findings, and other results of the

Medicare or private accreditation review applicable to the standards provided for in §438.204(g); and the District will provide the information to the EQRO.

Dually Eligible Beneficiaries Only

In accordance with §438.350(c) for MCOs serving only dually eligibles, the District will require MCOs to use the information produced by the District, its agent, or EQRO with respect to the mandatory activities in §438.358(b)(1) and (b)(2) instead of exercising the provisions of this standard. MCOs will continue to be responsible for providing the District all reports, findings, and other results of the Medicare review from all EQRO and EQR-related activities.

6. State Monitoring and Evaluation

Fraud, Waste, and Abuse: Each MCO must submit a written fraud, waste, and abuse compliance plan to MAA for approval. MAA received a written fraud, waste, and abuse compliance plan from all participating MCOs. MAA also developed a formal plan for preventing, detecting, pursuing, and reporting fraud, waste, and abuse in the managed care program, which identifies the staff, systems, and other resources devoted to this effort.

MAA is committed to the successful prevention and detection of fraud, waste, and abuse in the Medicaid program. The Office of Program Integrity (OPI) is the mandated entity that is responsible for the detection and prevention of Medicaid fraud, waste, and abuse. Specifically, two branches within OPI have the primary responsibility for carrying out these activities: (1) Investigations and Compliance Branch, and (2) Surveillance and Utilization Review Branch. In addition, the Office of Managed Care also plays a role with the collection of encounter data, monitoring the MCO contracts, conducting MCO readiness reviews, and monitoring the EQRO contract.

MAA is always trying to be a better purchaser of health care services by addressing fraud, waste, and abuse issues up front and by contracting only with MCOs that meet its standards and requirements for participation in the Medicaid program. Proper contracting provisions, quality assurance mechanisms, and audits are in place to ensure that MCOs comply with Federal and local laws and regulations as well as being accountable for their activities. To increase the likelihood of early identification and prevention of fraud, waste, and abuse, the OPI's monitoring and enforcement activities will include the following:

a. Review MCO contracts;
b. Review MCOs Marketing Plans and Materials;
c. Review MCOs Quality Assessment and Continuous Quality Improvement Programs;
d. Review MCOs Service Authorization Policies;
e. Review MCOs Providers Network Adequacy;
f. Conduct annual managed care fraud and abuse training; and
g. Review and Monitor MCOs Fraud and Abuse Compliance Plans

It is important that each MCO assesses its own organization and determines its needs concerning compliance with applicable Federal and District laws and health care program requirements.

7. Procedure for Race, Ethnicity, and Primary Language

Medicaid captures recipient race/ethnicity information during the eligibility determination process. The data are transmitted from the Income Maintenance Administration's Automated Client Eligibility Determination System (ACEDS) regularly as the entire recipient eligibility file is transposed to MAA's MIS system. The information is then sent monthly to then MCOs and rosters are generated and posted. MAA plans to use its MIS system to capture the primary spoken language during the Medicaid certification process.

8. National Performance Measures and Levels

MCOs must generate and track the performance measures as described within the contract and those that are mandated by the Centers for Medicare and Medicaid Services or other Federal and District governmental entities. Also, in accordance with 42 CFR 438.240, the MCO must have an ongoing program of performance improvement projects, which focus on clinical and non-clinical areas. The status of these performance improvement projects must be reported to the District as requested.

9. Intermediate Sanctions

MCOs that fail to comply with the terms and requirements of the contract and in accordance with 42 CFR 422.208 (a)-(h) regarding the physician incentive plan will be subject to intermediate sanctions.

D. Additional Information Related to Access to Care and Persons with Special Health Care Needs

1. Promote and Monitor Access to Services

MCOs must provide access to services for its Medicaid beneficiaries. For example, MCOs are required to:

a. Accept enrolled or assigned beneficiaries;
b. Contract and maintain a network of providers, including preventive, primary care, emergency/urgent, specialty, and ancillary providers in underserved areas, who provide items and services included in covered benefits;
c. Provide transportation from beneficiary’s home to medical care settings;
d. Offer language interpretation and services for sensory impaired beneficiaries;
e. Ensure access to timely appointments and after-hours access; and
f. Provide outreach and case management services.

The District is obligated to oversee, monitor, and evaluate MCOs on a host of activities related to access to services. The District’s EQRO evaluates the

beneficiaries' rights and responsibilities under each MCO/special health plan, including the access and availability provided to beneficiaries. Overall, the service standards are monitored on a monthly, quarterly, or annual basis and may include the following:

a. GEO Access Mapping based on zip code, mileage, and travel time analysis to identify any gaps in access to primary care providers, specialty providers, and pharmacies;
b. Additional evaluations include: utilization of non-participating providers, terminations or failure to apply for network recredentialing; MAA contractual requirements, member/provider requests;
c. Appointment times for comprehensive initial examination and follow-up on physical examination;
d. Average wait-times in PCP offices;
e. Non-emergent referrals for specialist appointments;
f. Average time to schedule urgent/emergent appointments;
g. Initial health screens under EPSDT guidelines;
h. Access to after-hours care;
i. Office responsiveness/telephone responsiveness;
j. Corrective action plans for identified gaps/deficiencies;
k. Evaluation of member complaints related to access and services;
l. Any physician office access issues (e.g., barriers to American with Disabilities Act, privacy information) during the onsite review of physician office setting;
m. Evaluation of emergency room use to identify patterns by time of day, practitioner, geographic area, zip code, and service gap;
n. Use of different languages spoken by providers in the network; and
o. Use of limited English proficiency beneficiaries.

MAA will work with MCOs to develop a series of programs to improve access to providers and support services for all beneficiaries. Specifically, MAA will work with MCOs to define access in real terms (i.e., measuring accessibility); to develop strategies to find and contract with providers in geographic and clinical areas that are underserved; to install providers and foster contracting (including community health clinics); to implement creative solutions for bridging the gap between beneficiaries and providers (such as mobile vans to get to providers), to evaluate plan networks for credentialing, recredentialing, wheelchair accessibility, and equipment for EPSDT; and to assign responsibilities between MAA and MCOs to measure and monitor access issues..

2. Promote and Monitor Services to Special Health Care Needs Populations

MCOs are required to ensure that children and adults with special health care needs have access to and appropriate use of integrated, comprehensive, community-based, quality health services. In accordance with 42 CFR 438.208 (c) (2-4), MCOs must maintain a case management system, including utilization management and care coordination that ensures that all beneficiaries are regularly examined to identify potential or actual health problems requiring

prevention, treatment, rehabilitation, and/or education in self-care. This system must be operated in accordance with applicable standards for high quality provision of services, including EPSDT, IDEA, standards for prenatal care, and relevant professional standards for the provision of health care to adults. In addition, MCOs must implement mechanisms to assess each Medicaid beneficiary identified by the District or by the MCO itself as having special health care needs in order to identify any ongoing special conditions of the beneficiary that require a course of treatment or regular care monitoring. The assessment mechanisms shall use appropriate health care professionals.

For the District, special needs populations include:

a. Persons living with HIV/AIDS, special heath care needs, or other disabling conditions with a cognitive, biological, or psychological basis that require special or complex medical, assistive, or personal accommodations;
b. Persons in need of mental health and substance abuse services; and
c. Children who are at risk for chronic physical, developmental, behavioral, or emotional conditions and who require health and related services of a type or amount beyond those required of children generally.

Special needs populations may also include:

a. Adolescents or women with high-risk pregnancies;
b. Beneficiaries with complex disease management issues or complex psychological needs which could adversely affect their health status;
c. People with or at-risk of serious life threatening conditions;
d. Children with mental health care needs;
e. Persons covered under the Individual with Disabilities Education Act (IDEA);
f. SSI or SSI-related children; and
g. Persons with limited English proficiency (LEP), self-identified as having a disability, or have seen a specialist more than three times in the last year.

MAA and EQRO representatives review each MCO's internal continuous quality improvement plan to ensure that policies and procedures are established for working with special populations. The plan must show that the infrastructure of the MCO is sufficient to satisfy the coordination requirements outlined in the MCO contract, including the provision of case management services for children with developmental delays and persons with HIV/AIDS. Thereafter, the District's EQRO representatives perform an annual review of each MCO. During this review, the District's EQRO representative assesses the MCO's internal continuous quality improvement plan. One component of the annual EQRO survey is an assessment of whether the MCO has a mechanism for identification of special groups that have unique health problems. EQRO looks for three elements to determine if this system is operational. First, beneficiaries with special health care needs must be enrolled in case management services according to established criteria and receive the appropriate care. Second, the MCO must have policies and procedures to coordinate care with other appropriate agencies or institutions. Third, the MCO must monitor continuity of care across all services and treatment modalities. To improve results, a

corrective action plan (CAP) is required of the MCO. The corrective action plan is developed under the direction of MAA and EQRO. Lastly, MAA and EQRO representatives meet monthly and/or quarterly, as deemed necessary, with the director of quality from each MCO in an effort to proactively monitor program performance and to explore best treatment clinical practices for implementation.

MAA places emphasis on increasing EPSDT screening rates and ensuring the completion of all components of the EPSDT screen, including a physical and mental health assessment. This assessment will ensure identification of children with special health care needs, and ensure appropriate referrals for corrective treatment. EPSDT will continue to be used as a performance measure for quality and access for special needs children.

As a clinical continuous quality improvement initiative, MCOs will be required to develop a method for tracking and identifying children with special health care needs on their information system to analyze utilization and health outcomes data for their special population. Results of the tracking and analysis will be presented to MAA and will be used by MCOs to develop clinical continuous quality improvement projects (approved by MAA and CMS, as appropriate) specifically for children with special health care needs. This activity is slated to be performed during the second six (6) months of the MCO second contract year.

The State and Local Integrated Telephone Survey (SLAITS) sponsored by the Centers for Disease Control and Prevention (CDC and Prevention) is a large, stratified random survey (over 900,000 interviews annually) that collects information from parents regarding their children's immunizations. The most recent SLAITS survey included a special module targeted on children with special needs that included questions in the following areas:

a. Health and functional status;
b. Access to care and unmet needs;
c. Care coordination and satisfaction with care;
d. Health insurance and health care coverage adequacy;
e. Income/household data;
f. Medicaid/SCHIP knowledge; and
g. Barriers for low income/uninsured children with special health care needs.

The SLAITS Special Health Care Needs Module (SLAITS Module) includes statistically valid samples from all states, including the District and samples families that are and are not Medicaid eligible. The District hired a private contractor (Abt Associates) to conduct an independent evaluation of its Medicaid Managed Care Program, including an analysis using the SLAITS Module that compared the District's children with special needs population with corresponding populations in Maryland, Virginia, and the nation. Results from the SLAITS Module analysis will be reported as part of the Plan for the first year.

Currently, MAA is in the process of expanding the composition requirements for the MCO Medicaid Advisory Committee to ensure representation of populations with special health care needs. MAA has enlisted the support of over 100 organizations to assist with its outreach efforts including advocates of children

with special health care needs (Children's Defense Fund, Children's Health Care Coalition of DC, Hope for Kids, Children with Special Health Care Needs Advisory Board, and Maternal and Family Health Administration), persons with HIV/AIDS, and the Seriously Persistently Mentally Ill (SPMI).

MAA will work with MCOs to develop programs that target the special needs populations that help identify individuals and their needs (i.e., Child and Adolescent Health Measurement Initiative (CAHMI) – a screening instrument), and facilitate the development of appropriate interventions and wrap-around programs between MCOs and the District schools. MAA will also evaluate the impact of policy and contextual changes on the District's special needs population and work to develop alternative policies to promote optimal service and support to MCOs.

3. Ensure Compliance with EPSDT Requirements

EPSDT is the pediatric component of the Medicaid program created and implemented by Federal statute and regulations. It is a program that establishes standards of care for children and adolescents under age 21, calling for regular screenings and services needed to prevent, diagnose, correct, maintain, or ameliorate a physical or mental illness. Contractually, MCOs are responsible for coverage and provision of health care, diagnostic services, treatment and other items described under the Federal law to address physical and mental illnesses and conditions discovered by the EPSDT screening services in the target population. If services are specifically excluded from MCOs' contract but are covered under the Medicaid fee-for-service, MCOs are still responsible for the treatment services and for coordinating care for the beneficiary, but not for the cost of providing the treatment services.

MCOs must ensure that network primary care providers perform comprehensive EPDST screenings and participate in the Vaccines for Children initiative. Additionally, MCOs must develop an outreach plan that describes their outreach efforts and activities directed to track and promote compliance with EPSDT periodicity schedules. The outreach plan is to be reviewed and updated by MCOs annually.

To coordinate health services for children that are serviced by other children's health care agencies and to address EPSDT, MAA integrated an interagency memorandum of understanding (MOU) with ten (10) District agencies/programs for the purpose of coordinating improved access to high quality mental health services. These MOUs provide a framework for working with beneficiaries and their advocates and stakeholders to ensure that mental health services are delivered in a manner that promotes integrated community-based services.

These entities include:

a. District of Columbia Public Schools (DCPS)
b. District of Columbia, Health and Human Services, Office of Early Intervention

c. District of Columbia Public School Head Start
d. United Planning Organization Head Start
e. District of Columbia Child and Family Services
f. District of Columbia Youth Services
g. Maternal and Family Health Administration (MFHA)
h. Office of Lead Poisoning Prevention
i. Addictions Prevention and Recovery Administration (APRA)
j. District of Columbia Court System
k. Department of Mental Health

MCOs are required to submit to MAA quarterly and annually reports detailing by age the number of EPSDT beneficiaries in the MCO who received screens, corrective actions, referrals, or treatments coupled with information on immunizations. In response to the variation in EPSDT screening ratios reported since FY 1994, MAA established a multifaceted approach to improve EPSDT reporting compliance. Firstly, in an attempt to make the program more readily acceptable by the Medicaid population, the EPSDT program changed its monitoring instrument to the HealthCheck Tracking System (HealthCheck). Using the HealthCheck instrument was an effort to close gaps in the reporting requirements as well as for continuous quality improvement purposes. MAA launched a District-wide campaign to capture EPSDT service information accurately at the point of encounter through the HealthCheck. A collaborative effort consisting of MAA representatives, MCOs' beneficiaries, and staff from other Department of Health agencies helped provide input into the development of the HealthCheck Tracking System. This universal database is a form-based process that uses a universal 'encounter' form. The form, used by providers, simplifies and accurately quantifies EPSDT service information. Since August 2002, the form underwent a pilot phase and is currently in use District-wide. As of April 2003, approximately 2000 forms were in the tracking system and close to 50 providers actively used the form.

Secondly, EPSDT reporting in the District was problematic in that each MCO plan had its own unique information systems with specific policies and procedures for data capturing and reporting. The variation in data collection methodologies among plans made it difficult for MAA to reconcile reports received from MCOs. To address this issue, MAA recently established a data analysis committee with representation from all MCOs and EQRO to improve the quality, accuracy, and reliability of the data and the reporting process.

Thirdly, improvements to EPSDT provider training continue to be implemented. An online provider training system is in development along with education modules specific to EPSDT reporting and clinically appropriate service guidelines. This initiative evolved from the October 2000 provider survey that indicated a lack of adequate EPSDT training and the providers' need for more information. The web-enabled training system is projected for availability to providers in mid-2004. MAA strengthened its EPSDT monitoring requirements and introduced disincentives for non-compliance. Thus far, the District's EQRO completed an EPSDT focused review. During this review, the EQRO's tracking system determined that MCOs were compliant with all required components of

the review, including comprehensive well-child examinations that include detailed health and mental health assessments.

Finally, MAA and EQRO will work with MCOs to develop a set of interventions specifically focused on solving issues identified under court monitoring and EPSDT services.

E. Additional Information Related to Structure and Operations Standards

1. Organizational Standards

Under the terms and conditions of the contract, an MCO must have a well-defined organizational structure with clearly assigned responsibility and accountability for major managed care functions. The MCO organizational structure must include the following as part of its executive management team:

a. A Chief Executive Officer with clear authority over the entire operation and a designated Senior Manager with overall responsibility for fulfilling the terms of the contract.

b. A Chief Financial Officer to oversee the budget and accounting system.

c. A board-certified physician licensed in the District with at least five years experience to serve as Medical Director for the MCO and PIHP (CASSIP) programs. The responsibilities of the Medical Director pertain to physical health care inclusive of the following functions:

   i. Development of clinical practice standards, policies, procedures, and performance standards;
   ii. Review and resolution of quality of care problems including the participation in grievance and appeal processes related to service denials and clinical practice;
   iii. Development, implementation, and review of the internal continuous quality improvement and utilization management programs;
   iv. Oversight of the referral process for specialty and out-of-plan services;
   v. Leadership and direction for the MCO's clinical staff recruitment, credentialing, recredentialing, and privileging activities;
   vi. Leadership and direction for the MCO's prior authorization and utilization review process;
   vii. Leadership and direction of policies and procedures relating to confidentiality of clinical records; and
   viii. Participation in meetings sponsored by MAA.

The MCO organizational structure must include the following personnel:

a. Senior Manager, who may or may not be the contracted Psychiatric Medical Director, with overall responsibility for performance of the MCO's obligations to provide mental health, alcohol and drug abuse services, and to coordinate

activities as appropriate with the Department of Mental Health and the Addiction Prevention and Recovery Administration;

b. A Senior Manager with overall responsibility for a Continuous Quality Improvement Program to assess ongoing quality and to develop and implement the MCO's Continuous Quality Improvement Plan;

c. A Senior Manager with overall responsibility for a Care Coordination Program to coordinate care for beneficiaries with multiple, complex and/or intensive treatment needs including individuals in need of alcohol and drug abuse treatment services;

d. A Senior Manager with overall responsibility for a Member Services Program to communicate with beneficiaries on a twenty-four (24) hours per day, seven (7) days per week basis, who acts as a member advocate, and who coordinates members' use of the complaint, grievance, and appeals processes;

e. A Senior Manager with overall responsibility for a Provider Services Program to coordinate communications between the MCO and its providers and oversees provider network management; and

f. A Senior Manager with overall responsibility for Management Information Services to support the operations of computerized systems for collection, analysis and reporting of information.

The MCO must establish a Medicaid Advisory Committee within sixty (60) days of the contract award. The MCO must ensure that this committee meets at least quarterly to advise MCOs on matters relating to services to beneficiaries. The Medicaid Advisory Committee must also include network providers, beneficiaries, and sufficient other stakeholders representative of relevant advocacy groups, trade associations, and the District agencies that serve Medicaid managed care beneficiaries to provide comprehensive feedback on the MCO's operations and planned changes. MAA will approve the overall representation on the committee and the scope of its jurisdiction.

MCOs must generate and maintain minutes and records of the agendas of meetings, issues raised, and any recommendations made to resolve identified issues or to improve the MCOs' operations. These records must be available within three (3) working days of each meeting and may be reviewed by MAA or its representative(s), upon request.

In terms of marketing, the MCO can engage in permissible marketing activities and develop marketing materials and information within the terms and conditions of the MCO contract and the applicable District and Federal regulations and statutes.

2. Decision Resolution Processes

The decision resolution process must include both informal and formal provisions for resolving issues presented by a beneficiary or a provider associated with the plan.

a. Complaint Process (Informal)

Each MCO/PIHP must create an informal complaint procedure approved in writing by the District, which provides for prompt resolution of issues, and assures participation of individuals with authority to order corrective action. The procedure must allow a beneficiary or a provider on behalf of a beneficiary to challenge the denial of coverage of, or payment services as required by 1932(b) of the Act. A complaint may be presented verbally or in writing. The beneficiary or provider reserves the right to decide whether to seek resolution through the plan's complaint process before exercising the grievance and appeal provisions. The beneficiary or provider will not incur any reprisal for opting to utilize the grievance or appeal systems in lieu of the plan's complaint process. Each MCO must maintain an accurate record of all complaints logged upon receipt and provide a written notice of resolution to the beneficiary or provider within ten (10) days of receipt. MAA may request submission of the plan's complaint log to be released within three (3) days of notification.

b. Grievances and Appeals (Formal) – General Provision

The MCO must establish and maintain an appeals process to review and resolve the denial or limited authorization of requested service(s) resulting from the standard grievance process.

The MCO must reconsider a decision to deny, reduce, terminate, or delay authorization of a requested covered service or payment denial in response to a grievance request submitted by a beneficiary or a provider on behalf of a beneficiary. Should the beneficiary disagree with the MCO's response to a grievance, the beneficiary or a provider on the beneficiary's behalf may appeal the MCO's decision.

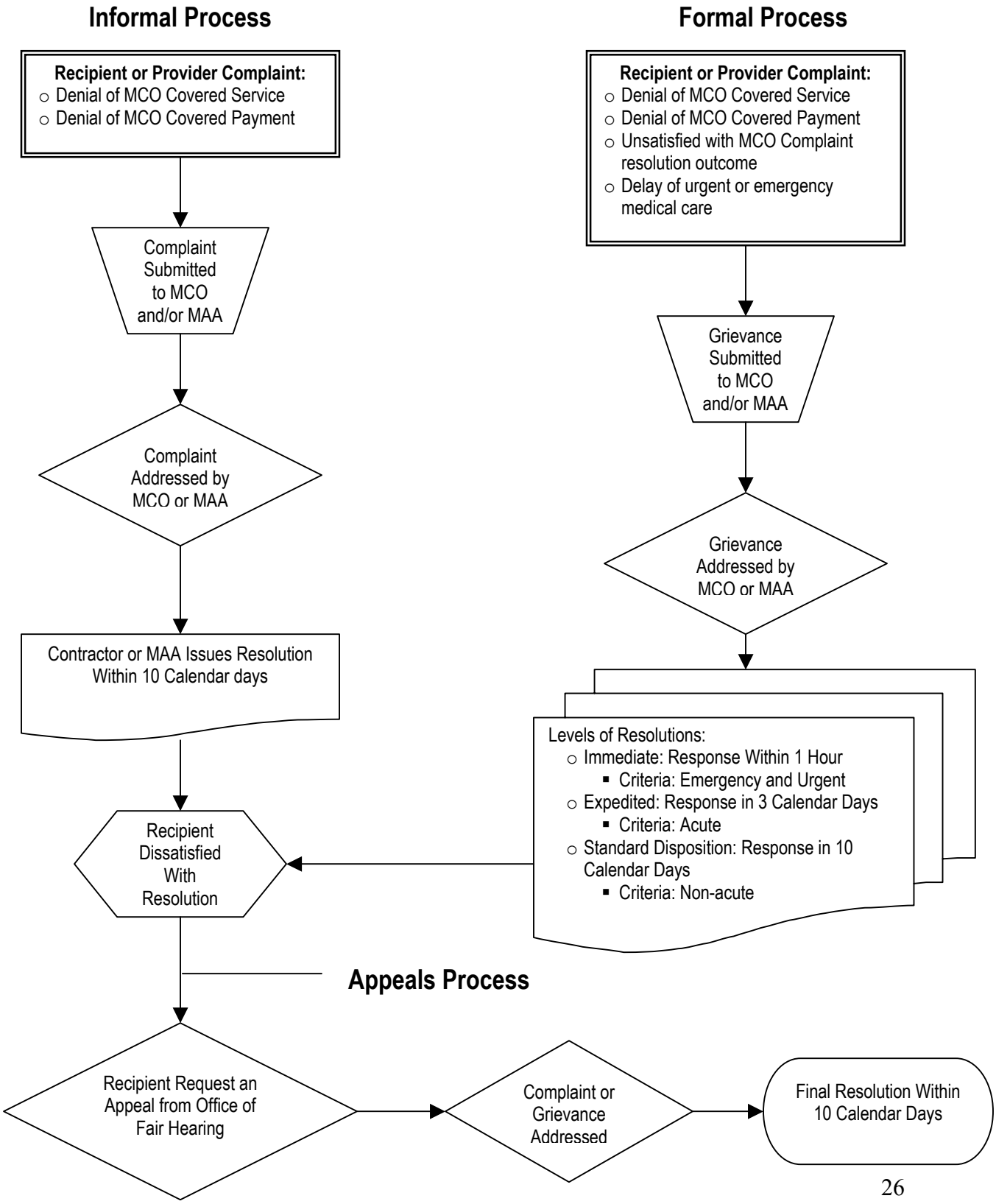
3. Levels of Reconsideration

The MCO must notify the beneficiary ten (10) business days prior to action whenever a beneficiary's request for covered services is delayed, reduced, denied, or terminated. In cases of service reduction, delay, denial or termination, the MCO must send a monthly report to the Office of Managed Care by the end of each month. For payment denials, the MCO must notify the provider and provide a monthly summary report to the Office of Managed Care by the end of each month.

In accordance with 42CFR 438.210(b)(3), any decision to deny a service authorization request or to authorize a service in an amount, duration, or scope that is less than requested, must be made by a health professional who has appropriate clinical expertise in treating the beneficiary's condition or disease.

EXHIBIT 1

Recipient and Provider Complaints, Grievances, and Appeals Decision Resolution Process



The notification must meet the requirements of 42 CFR 438.404 and include the following information:

a) The action the MCO or its subcontractor has taken;
b) The reason for the action;
c) The beneficiary's or the provider's right to file an MCO or CASSIP appeal;
d) The right to request a District Administrative Hearing immediately;
e) The procedures for exercising these rights;
f) The circumstances under which expedited resolution is available and how to request it; and
g) The beneficiary's right to have benefits continued pending resolution of the appeal, and how to request that benefits be continued.

4. Immediate Reconsideration

The MCO must establish a process for immediate reconsideration of the denial, termination, or reduction of services when there is a dispute about whether the beneficiary has an urgent or emergency medical condition or there is a delay in the furnishing of an emergency or urgent service. A physician not involved in the original decision must perform the review and reconsideration of the matter with a decision issued within a one (1) hour period of the request.

The MCO must utilize the immediate reconsideration process under the following circumstances:

a) A beneficiary (or designated representative as defined within the MCO contract) submits a grievance and taking the time for a standard resolution could seriously jeopardize the beneficiary's life or health;
b) A physician submits a grievance or supports a beneficiary's request and indicates that taking the time for a standard resolution could seriously jeopardize the beneficiary's life, health, or functioning; or
c) A beneficiary submits a grievance while accessing services for urgent or emergency care.

5. Expedited Grievance (Acute Care Cases)

The MCO must establish an expedited grievance process for making a first level reconsideration determination of an acute care denial within a seventy-two (72) hour period. The reviewer must be an appropriate specialist who was not involved in the initial coverage determination. Aggrieved individuals must have the right to submit additional data and meet with the reviewer prior to final determination.

In accordance with 42 CFR 438.410(b), the MCO must ensure that punitive action is neither taken against a provider who requests an expedited resolution or supports a beneficiary's appeal.

In accordance with 42 CFR 438.410(c), if the MCO denies a request for expedited resolution of an appeal, it must:

a) Transfer the appeal to the timeframe for standard resolution of an appeal; and
b) Make reasonable efforts to give the beneficiary prompt oral notice of the denial, and follow up within two (2) calendar days with a written notice.

The MCO must ensure that, at a minimum, the expedited grievance process is utilized for:

a) Persons dissatisfied with the response to a request for urgent care;
b) Persons with HIV/AIDS or with special health care needs dissatisfied with an MCO's determination of coverage;
c) Other persons as designated by the MCO based on stated criteria;
d) Persons who are dissatisfied with an MCO's determination of coverage for acute services or for services that may be authorized as alternatives to acute inpatient services; and
e) Persons dissatisfied with decisions regarding denial of surgical procedures, including but not limited to circumcisions.

6. Standard Disposition of Grievance (Non-Acute Cases)

The MCO must establish and maintain a standard grievance process for first level reconsideration of authorization decisions that resulted in the denial, termination, delay, or reduction of a covered item or service. This process may also serve as a first level reconsideration of an unresolved complaint/grievance, and resolved in ten (10) calendar days. The MCO must be responsible for the following activities regarding the grievance process:

a) The MCO must inform providers and beneficiaries of procedures for grievance denials or reductions of requested services.
b) The MCO must inform beneficiaries of their rights in the grievance process, including the right to appear in person before the MCO's personnel responsible for resolving the grievance **timing** in which the review will be completed and their rights to Administrative Hearings at any point in the process.
c) The MCO must ensure that appropriate pediatric specialists and sub-specialists review all grievances regarding services for children.
d) The MCO must appoint a Grievance Committee to review all standard grievances. At a minimum, the Grievance Committee must include the Medical Director or his/her designee, the Clinical Director or his/her designee, and a Supervising Care Coordinator representing a discipline other than the Clinical Director's. Other medical and clinical staff must participate or substitute for a staff member involved in the matter being grieved or to provide needed specialty expertise.
e) In accordance with 42 CFR 438.408(c), the time-frame can also be extended by up to fourteen (14) calendar days if the MCO shows to MAA's satisfaction, upon its request, that there is need for additional information and how the delay is in the beneficiary's interest. If the MCO

extends the timeframe, it must – for any extension not requested by the beneficiary - give the beneficiary written notice of the reason for the delay.

7. Appeals

The MCO must establish and maintain an appeals process to review and resolve disputes involving the denial or limited authorization of requested services resulting from the standard grievance process. MCOs must be responsible for ensuring:

a) The same resolution and notification timeframes (72 hours) and described above for the standard grievance process are adhered to throughout the appeals process.
b) The appeals committee responsible for the review and reconsideration of the dispute includes a physician who was not involved in any previous decision regarding the dispute.
c) In accordance with 42 CFR 438.406(b), the process for appeals must:

    i. Provide that oral inquiries seeking to appeal an action are treated as appeals (to establish the earliest possible filing date for the appeal) and must be confirmed in writing, unless the beneficiary or provider requests expedited resolution;
    ii. Provide the beneficiary a reasonable opportunity to present evidence, and allegations of fact or law, in person as well as in writing. The MCO must inform the beneficiary of the limited time available for this in the case of expedited resolution;
    iii. Provide the beneficiary and his or her representative the opportunity, before the appeals process, to examine the beneficiary's case file, including medical records, and any other documents and records; and
    iv. Include as parties to the appeal the beneficiary and his or her legal representative or the legal representative of a deceased beneficiary's estate.

d) The written notice of the resolution must include the following:

    i. The results of the resolution process and the date it was completed; and
    ii. For appeals not resolved wholly in favor of beneficiaries:
        - The right to request a District Administrative Hearing and how to do so; and
        - The right to request and receive benefits while the hearing is pending and how to make the request.

7. Timeframe for Filing Grievances

In the case of the issuance of a determination involving the denial of, or the termination or reduction of a covered item or service, any individual described in paragraph (1) may file a grievance within ninety (90) days of receipt of the notice.

An MCO must resolve grievances filed under this section no later than fourteen (14) working days after the date of receipt of the grievance, with the possibility of an extension of fourteen (14) days if it is in the best interest of the beneficiary, except in cases where the expedited grievance process is applicable.

If the MCO or PIHP extends the timeframe, the MCO or PIHP must give the beneficiary written notice of the reason for the decision to extend the timeframe and inform the beneficiary of the right to file a grievance if he or she disagrees with that decision; and issue and carry out its determination as expeditiously as the beneficiary's health condition requires and no later than the date the extension expires.

8. Requirements for Notice of Action

The MCO must notify a beneficiary in writing and in a timely manner of any intention to deny, limit, reduce, delay, or terminate a service or deny payment. This notice must clearly explain the following:

a) The action the MCO intends to take and the supporting reasons, laws, or rules for the action;
b) The beneficiary's right to file a complaint or grievance with the MCO and the right to request an Administrative Hearing at any time;
c) The beneficiary's right to appear in person in front of the MCO's personnel if the beneficiary files a grievance;
d) The beneficiary's right to have a representative involved in the process;
e) The assistance that can be provided by the Ombudsman and how to contact the Ombudsman;
f) The beneficiary's right to obtain free copies of the documents, including the beneficiary's medical records used to make the decision and the medical necessity criteria referenced in the decision;
g) In accordance with 42 CFR 438.404 and 438.210, the MCO, or PIHP gives notice as expeditiously as the beneficiary's health condition requires and within District-established timeframes that may not exceed fourteen (14) calendar days following receipt of the request for services. There is a possible extension of up to fourteen (14) additional calendar days, if the beneficiary or the provider requests the extension or the MCO or PHIP justifies a need for additional information and how the extension is in the beneficiary's interest. If the MCO or PHIP extends the timeframe, the MCO must give the beneficiary written notice of the reason for the decision to extend the timeframe and inform the beneficiary of the right to file a grievance if he or she disagrees with that decision; and issue and carry out its determination as expeditiously as the beneficiary's health condition requires and no later than the date the extension expires.
h) In accordance with 42 CFR 438.404(c), the MCO must mail the notice within the following timeframes:

    i. For termination, suspension, or reduction of Medicaid services, the timeframes specified in 42 CFR 431.211, 431.213, and 431.214;
    ii. For denial of payment at the time of any action affecting the claim;
    iii. For standard service authorization decisions that deny or limit services, within five (5) days.

If the MCO extends the timeframe in accordance with 42 CFR 438.210(d)(1), the MCO must:

a) Give the beneficiary written notice of the reason for the decision to extend the timeframe and inform the beneficiary of the right to file a grievance if he or she disagrees with that decision; and
b) Issue and carry out its determination as expeditiously as the beneficiary's health condition requires and no later than the date the extension expires.

For service authorization decisions not reached within the timeframe specified in 42 CFR 438.210(d) (which constitutes a denial and is thus an adverse action), on the date that the timeframes expire; and

In accordance with 42 CFR 438.404(b)(6), the circumstances under which expedited resolution is available and how to request it, for cases in which the provider indicates or the MCO or PHIP determines, that following the standard timeframe could seriously jeopardize the beneficiary's life or health or ability to attain, maintain or regain maximum function, the MCO or PHIP giving notice must make an expedited authorization decision and provide notice as expeditiously as the beneficiary's health condition requires and no later than the seventy-two (72) hours after receipt of the request for service, as specified in 42 CFR 438.210(d). The MCO or PHIP may extend the seventy-two (72) hour time period by up to fourteen (14) calendar days if the beneficiary requests an extension, or if the MCO or PHIP justifies a need for additional information and how the extension is in the beneficiary's interest.

9. Written Notification of Receipt

The MCO must, within two (2) working days, send to the beneficiary or the beneficiary's designee a letter of notification of receipt of the complaint or grievance.

10. Continuation of Coverage

In accordance with 42 CFR 438.420, the MCO must continue the beneficiary's benefits if:

a) The beneficiary or provider files a timely appeal;
b) The appeal involves the termination, suspension, or reduction of a previously authorized course of treatment;
c) The services were ordered by an authorized provider;
d) The original period covered by the original authorization has not expired; and
e) The beneficiary requests extension of benefits.

"Timely" means filing on or before the later of the following: (1) within ten (10) days of the MCO's mailing the notice of action; and (2) the intended effective date of the MCO's proposed action.

If the beneficiary requests that the MCO continues or reinstates benefits while the appeal is pending, the benefits must continue until one of the following occurs:

a) The beneficiary withdraws the appeal;
b) Ten (10) days pass after the MCO mails the notice, providing the resolution of the appeal against the beneficiary, unless the beneficiary, within the ten (10) days timeframe, has requested a District Administrative Hearing with continuation of benefits until a District Administrative Hearing decision is reached;
c) The District Office of Administrative Hearing issues a hearing decision adverse to the beneficiary; or
d) The time period or service limits of a previously authorized service has been met.

If the final resolution of the appeal is adverse to the beneficiary, that is, upholds the MCO's action, the MCO may not recover the cost of the services furnished to the beneficiary while the appeal is pending, to the extent that they were furnished solely because of the requirements of this contract and in accordance with the policy set forth in 42 CFR 431.230(b).

The MCO must issue an authorization for any services authorized as a result of the grievance or administrative hearing process within two (2) working days of a grievance or notice of an administrative hearing decision.

The MCO is prohibited from recovering payment for continuation of benefits furnished during a pending appeal, if the final resolution of the appeal is adverse to the beneficiary.

In accordance with 42 CFR 438.424, if the MCO or District Office of Administrative Hearing reverses a decision to deny, limit, or delay services that were not furnished while the appeal was pending, the MCO must authorize or provide the disputed services within two (2) working days of the decision, and as expeditiously as the beneficiary's health condition requires. In addition, if the MCO or District Office of Administrative Hearing reverses a decision to deny authorization of services, and the beneficiary received the disputed services while the appeal was pending, the MCO or PIHP must pay for those services, in accordance with District policy and regulations.

11. Administrative Hearings

The MCO must notify the beneficiary or the beneficiary's designee of the right to an administrative hearing with a District Administrative Hearing Officer each time notification of an adverse decision on a complaint, grievance, or appeal is sent.

In accordance with 42 CFR 431.220, the District shall grant an opportunity for a hearing to the following:

a) Any applicant who requests one because his/her claim for services is denied or is not acted upon with reasonable promptness; and

b) Any beneficiary who is the subject of an action or a grievance as defined in the contract.

The MCO must submit all documents regarding the plan's action and the beneficiary's dispute to MAA no later than five (5) working days from the date the MCO receives notice from the District that an Administrative Hearing request is filed at the beneficiary's request.

A beneficiary may request an administrative hearing before, during, or after an MCO's grievance process. However, a beneficiary is allowed no more than ninety (90) days from the date notice of action is mailed to request a hearing.

Pending the decision from the administrative hearing, the MCO must continue to furnish the item or service at the level and in the amount, scope, and duration that item or service was provided to the beneficiary prior to notification of the MCO's determination.

The MCO must assist the beneficiary with filing of any request for an Administrative Hearing and send a copy of the request filed to the beneficiary's home address.

12. Grievance and Administrative Hearing Resolutions

If the MCO reverses or modifies an authorized decision through the grievance resolution process or is notified of the District's Administrative Hearing decision to reverse a decision, the service must be authorized or provided no later than two (2) working days after reversal or notification of reversal from the District. In the case of an expedited grievance, services must begin within twenty-four (24) hours of the reversal.

The MCO must comply with the Office of Managed Care and the Office of Administrative Hearing decisions. The Office of Managed Care and the Office of Administrative Hearing decisions in these matters shall be final and shall not be subjected to appeal by the MCO. The MCO must provide to the Office of Managed Care and/or Office of Administrative Hearing all information necessary for any beneficiary appeal within a time frame established by Office of Managed Care and/or the Office of Administrative Hearing.

In accordance with 42 CFR 431.244, the hearing recommendations must be based exclusively on evidence introduced at the hearing.

The hearing record must consist only of the following:

a) The transcript or recording of testimony or exhibits or an official report containing the substance of what happened at the hearing;
b) All papers and requests filed in the hearing; and
c) The recommendation or decision of the hearing officer

The applicant or beneficiary must have access to the record at a convenient place and time.

In any evidentiary hearing, the decision must be a written one that:

a) Summarizes the facts; and
b) Identifies the regulations supporting the decision.

In a *de novo* hearing (i.e., a hearing that starts over from the beginning), the decision must:

a) Specify the reasons for the decision; and
b) Identify the supporting evidence and regulations.

VI. Conclusion

MAA has an ongoing responsibility to seek and nurture opportunities to provide and improve the health care and services to residents of the District of Columbia under the Medicaid managed care program. The program's mission and vision are challenged by many demands the District's government inherited. No demand, however, is more essential than ensuring, through the collaborative efforts of MAA, District's Medicaid MCOs, and other state, local and community agencies, that access to quality health care is available to the Medicaid population and that beneficiaries are satisfied with the managed care program.

Lastly, the Continuous Quality Improvement Plan for the Office of Managed Care will be revised, as necessary. An updated Plan will be submitted to the U. S. Department of Health and Human Services, Centers for Medicare and Medicaid Services within thirty (30) days of approval of any revisions by the District of Columbia, Medical Assistance Administration.

Definitions

Abuse: Any practice that is not consistent with the goals of providing beneficiaries with services which are: (1) medical necessary, (2) meet professionally recognized standards, and (3) are unfairly priced. Examples of abuse could be a range of the following improper behaviors or billing practices including, but not limited to:

- Billing for a non-covered service;
- Misusing codes on the claim (i.e., the way the service is coded on the claim does not comply with national or local coding guidelines or is not billed as rendered); or
- Inappropriately allocating costs on a cost report.

ACEDS: Automated Client Eligibility Determination System. The information system maintained by the District to document Medicaid claims payment and service provisions.

Action: The denial or limited authorization of a requested service, including the type or level of service;

- The denial in whole or in part of payment for a service;
- The failure to provide services in a timely manner as defined by the District; or
- The failure of the Contractor to act within the timeframes for resolution and notification of appeals and grievances in this section.

Actuarially equivalent: Costs the same.

Addictions, Prevention and Recovery Administration (APRA): The District of Columbia's agency responsible for alcohol and drug abuse treatment and prevention services, under the auspices of the Department of Health.

Adjudicated Claim: A claim that has been processed for payment or denial.

Administrative Cost: All operating costs of the Contractor, including care coordination, but excluding medical costs.

Administrative Hearing, formerly Fair Hearing: The process adopted and implemented by the Government of the District of Columbia, Department of Health in compliance with Federal regulations, States and District rules relating to Medicaid Fair Hearings found at 42 CFR Part 431, Subpart E.

Adults with Special Health Care Needs: Adults who have an illness, condition or disability that results in limitation of function, activities or social roles in comparison with accepted adult age-related milestones in general areas of physical, cognitive, emotional, and/or social

growth and/or development, or people who have seen a specialist more than three (3) times in the last year. This definition includes but is not limited to individuals who self-identify as having a disability or who meet the standard of limited English proficiency, or have seen a specialist more than three times in the last year.

Advance Directive: A written instruction, such as a living will or durable power of attorney for health care, recognized under State law (whether statutory or as recognized by the courts of the State), relating to the provision of health care when the individual is incapacitated.

Affiliate: Any individual, corporation, partnership, joint venture, trust, unincorporated organization or association, or other similar organization (hereinafter "Person"), controlling, controlled by or under common control with Contractor or its parent(s), whether such common control be direct or indirect. Without limitation, all officers, or persons, holding five percent (5%) or more of the outstanding ownership interests of Contractor or its parent(s), directors or subsidiaries of Contractor or parent(s) shall be presumed to be affiliates for purposes of the RFP and Agreement. For purposes of this definition, "control" means the possession, directly or indirectly, of the power (whether or not exercised) to direct or cause the direction of the management or policies of a person, whether through the ownership of voting securities, other ownership interests, or by contract or otherwise including but not limited to the power to elect a majority of the directors of a corporation or trustees of a trust, as the case may be.

Alcohol and Drug Abuse Treatment Services: Care and services which are covered under the District of Columbia Medicaid plan or that are otherwise furnished to District residents pursuant to any other funded programs and which are required for the diagnosis and treatment of an illness or condition which is classified as an addiction-related disorder under the ICD-9 or DSM-IV.

Alternate Payment Name: A person to whom benefits are issued on behalf of a beneficiary.

American Accreditation Health Care Commission/URAC: Commission that establishes accreditation standards for managed care organizations.

Appeal: An application for review by a higher tribunal (in a legislative body or assembly) a formal question as to the correctness of a ruling by a presiding officer (A Formal Process).

Authorization: See Prior Authorization, Service Authorization.

Automatic Enrollment: A process for assigning beneficiaries to a health plan if they have not exercised their right to choose for themselves within the allowed time frame.

Beneficiary: A Medicaid recipient who is currently enrolled in an MCO or CASSIP participating in the District of Columbia's Medicaid managed care program.

Beneficiary Satisfaction Surveys: Valid and reliable surveys to measure beneficiaries' overall satisfaction with Medicaid services and with specific aspects of those services, in order to identify problems and opportunities for improvement.

Business Days: These include Monday through Friday except for those days recognized as Federal and/or District holidays.

Cancellation/termination: Discontinuation of the contract for any reason prior to the expiration date.

Capitation Payment: (OPTIONAL) A payment MAA makes periodically to a Contractor on behalf of each recipient enrolled under a contract for the provision of medical services under the District's plan. MAA makes the payment regardless of whether the particular recipient receives services during the period covered by the payment.

Care Coordination: Refers to the activities of assisting beneficiaries and service providers to coordinate care for beneficiaries with multiple, complex, and/or intensive treatment needs, including participating in assessments, treatment planning, making referrals, providing health education, facilitating exchange of information, monitoring implementation of treatment plans, discharge planning, and coordination. It also includes cooperating with other District agencies or entities serving beneficiaries, such as, but not limited to, the Department of Mental Health Services, Public Schools, and the District's Children and Family Services.

Care Management System: Refers to an organized system for managing the medical, mental health, alcohol and drug abuse and/or special needs of beneficiaries with complex health care needs, including Primary Care Physicians' responsibility for providing and managing primary care, an EPSDT tracking system, a utilization management system with special procedures for high cost/high-risk cases, and care coordination.

Case Management Services: Services which will assist individuals in gaining access to necessary medical, social, educational, and other services.

Case Payment Name: The person in whose name benefits are issued.

CASSIP: Child and Adolescent Supplemental Security Income (SSI) or SSI-related Plans means programs that meet the accreditation requirements of this contract and that have the required demonstrated experience in serving children and adolescents who

are SSI eligible or who have SSI related diagnoses and who have disabilities and complex healthcare needs.

Center for Medicare and Medicaid Services (CMS): The Federal agency within the U.S. Department of Health and Human Services responsible for oversight of Medicaid programs, formerly known as the Health Care Financing Administration (HCFA).

Certified Nurse Midwife: An individual licensed under the laws within the scope of the Act of April 04, 1929 [P.L. 160, NO.155].

Certified Registered Nurse Practitioner (CRNP): A registered nurse licensed in the District of Columbia who is certified by the Boards in a particular clinical specialty area and who, while functioning in the expanded role as a professional nurse, performs acts of medical diagnosis or prescriptions of medical therapeutic or corrective measures in collaboration with and under the direction of a physician licensed to practice medicine in the District of Columbia.

Child: Refers to children and adolescents ages 0 through 21 eligible for Medicaid and/or enrolled in a Medicaid Managed Care Program.

Children with Special Health Care Needs: Children who have, or are at increased risk for, chronic physical, developmental, behavioral, or emotional conditions or who also require health and related services of a type or amount beyond those required by children generally. This definition includes children on SSI, children who are SSI-related eligible, children who are or have been in foster care, and children who meet the standard of limited English proficiency, or have seen a specialist more than three times in the last year.

Claim: A bill from a provider of a medical service or product that is assigned a unique identifier (i.e. claim reference number). A claim does not include an encounter form for which no payment is made or only a nominal payment is made.

Clean claim: Claim submitted on an approved claim form, and containing complete and accurate information for all data fields required by the Contractor and MAA for final adjudication of the claim. If information that is not included on the claim form is necessary for adjudication of a claim, then such additional information shall be submitted as required in order for the claim to be considered "clean".

Closed Panel: A managed care plan that contracts with physicians on an exclusive basis for services and does not allow those physicians to see patients for another managed care organization. Examples include staff and group model HMOs. Could also apply to a large private medical group that contracts with an HMO.

Complaint: An issue a beneficiary or provider presents to the managed care organization, either in written or oral form, which is subject to resolution by the contractor, their designee, and/or MAA.

Competent Professional Interpreter: A person who is proficient in both English and the other language; has had orientation or training in the ethics of interpreting; has the ability to interpret accurately and impartially; and has the ability to interpret for medical encounters using medical terminology in English and the other language.

Comprehensive Risk Contract: A risk contract that covers comprehensive services, that is, inpatient hospital services and any of the following services or any three or more of the following services:

- Outpatient hospital services;
- FQHC services;
- Other laboratory and x-ray services;
- Nursing facility (NF) services;
- Early and periodic screening, diagnostic, and treatment (EPSDT) services;
- Family planning services;
- Physician services;
- Home health services; and
- Mental health services

Concurrent Review: A review conducted by the contractor or MAA during a course of treatment to determine whether or not services should continue as prescribed or should be terminated, changed, or altered.

Continuity of Care: Care provided to a beneficiary that is coordinated by a designated primary care provider or specialty provider to the greatest degree possible, so that the delivery of care to the beneficiary remains stable, services are consistent and unduplicated, and persons involved in the care and treatment of the beneficiary understand and support the plan of care.

Continuous Quality Improvement: Methods to identify opportunities for improving organizational performance, identify causes of poor performance, design and test interventions, and implement demonstrably successful interventions system-wide.

Contractor: A managed care organization participating in the District's Medicaid Managed Care Program authorized under DC Code sec. 1-359(d).

Covered Services: Health care services that the contractor shall provide to beneficiaries, including all services required by this contract and state and Federal law, and all additional services described by the contractor in its response to the Request For Proposal (RFP) for this contract.

Credentialing: A review process to approve a provider or professional who applies to provide care in a hospital, clinic, medical group, or health plan, based upon specific criteria, standards and prerequisites, including Federal health care program requirements (see also "Primary Source Verification").

Crisis Plan: A plan developed by the beneficiary, the beneficiary's family (when relevant), and the beneficiary's medical or mental health and alcohol or drug abuse providers to guide the management of medical or mental health/alcohol and drug abuse crises for which the beneficiary is at risk. In addition to conditions which meet the definition of emergency, mental health conditions which severely compromise an individual's ability to maintain his or her customary level of functioning or which put him or her at risk for harming self or others are also considered to be crisis situations.

Cultural and Linguistic Competence: A set of skills that allow service providers and medical organizations to respond sensitively and respectfully to people of various cultures, races, ethnic backgrounds, religions, and sexual preferences and to communicate with them accurately and effectively to identify and diagnose health-related problems and to jointly develop culturally appropriate plans for treatment and self-care.

Day: A calendar day, unless otherwise specified.

Deliverables: Records and reports required to be furnished to MAA for review and/or approval pursuant to the terms of the RFP and Agreement.

Denial of Services: Any determination made by the contractor in response to a provider's request for approval to provide MAA-covered services of a specific duration and scope which: disapproves the request completely; approves provision of the requested service(s), but for a lesser scope or duration than requested by the provider; or disapproves provision of the requested service(s), but approves provision of an alternative service(s). An approval of a requested service, which includes a requirement for a concurrent review by the contractor during the authorized period, does not constitute a denial.

Denied Claim: An adjudicated claim that does not result in a payment obligation to a provider.

Department of Mental Health: Refers to the Government of the District of Columbia agency responsible for mental health treatment and prevention services. This new agency is responsible for functions previously provided by the Commission on Mental Health/Dixon Transition Receiver.

Disease Management: An integrated treatment approach that includes the collaboration and coordination of patient care delivery systems

and that focuses on measurably improving clinical outcomes for a particular medical condition through the use of appropriate clinical resources such as preventive care, treatment guidelines, patient counseling, education, and outpatient care; and that includes evaluation of the appropriateness of the scope, setting, and level of care in relation to clinical outcomes and cost of a particular condition.

Disenrollment: Action taken by MAA to remove a member's name from the monthly Enrollment Report following MAA's receipt of a determination that the member is no longer eligible for enrollment.

District of Columbia Healthy Families Program (DCHFP): District of Columbia Healthy Families Program is the District's combination of the Medicaid program and the State Children's Health Insurance Program (SCHIP).

Developmental Disability: A severe, chronic disability that is (or is suspected of being):

a) Attributable to a mental or physical impairment or combination of mental and physical impairments;
b) Manifested before the individual attains age 22;
c) Likely to continue indefinitely; and that
d) Results in functional limitations or impairment of normal growth and development (if not treated); and
e) When applied to infants and young children with substantial developmental delay or specific congenital or acquired conditions, either result, or, if not treated, could result in developmental disabilities.

District: Refers to the Government of the District of Columbia.

DSM-IV: The Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition, which is the American Psychiatric Association's official classification of mental health and alcohol and drug abuse disorders.

Dual Eligibles: An individual who is eligible to receive services through both Medicare and Medicaid.

Early and Periodic Screening, Diagnosis, and Treatment (EPSDT): The pediatric component of the Medicaid program created and implemented by Federal statute and regulations. This program establishes standards of care for children and adolescents under age 21, calling for regular screening and for the services needed to prevent, diagnose, correct or ameliorate a physical or mental illness, including alcohol and drug abuse, or condition identified through screening. Medicaid services for children are required as a matter of law to meet these standards, which may require that services outside traditional Medicaid benefits be provided when needed to treat such conditions.

Eligibility Period: A period of time during which a beneficiary is eligible to receive MAA benefits. An eligibility period is indicated by the eligibility start and end date.

Eligibility Verification System (EVS): The information system maintained by the District of Columbia, Department of Human Services, Income Maintenance Administration that allows providers to verify eligibility status of Medicaid recipients.

Emergency Medical Condition: A medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) such that a prudent layperson, who possesses an average knowledge of health and medicine, could reasonably expect the absence of immediate medical attention to result in:

a) Placing the health of the individual (or, with respect to a pregnant woman, the health of the woman or her unborn child) in serious jeopardy;
b) Serious impairment to bodily functions; and/or
c) Serious dysfunction of any body organ or part.

Emergency Member Issue: A problem of a member (including problems related to whether an individual is a member); the resolution of which should occur immediately or before the beginning of the next business day in order to prevent a denial or medically significant delay in care to the member that could precipitate a medical emergency condition or need for urgent care.

Emergency Services: Covered inpatient or outpatient services that

a) Are furnished by an appropriate source;
b) Are needed immediately because of an injury or sudden illness; and
c) Cannot be delayed for the time required to reach the contractor without risk of permanent damage to the beneficiary's health.

Encounter Data: Any health care service provided to a member. Encounters whether reimbursed through capitation, fee-for-service, or another method of compensation shall result in the creation and submission of an encounter record to MAA. The information provided on these records represents the encounter data provided by the contractor.

Enrollment: The process by which a member's entitlement to receive services from a contractor is initiated.

Enrollment Broker: The contractor that provides assistance to Medicaid eligibles in the selection of a health plan. The same contractor will offer a 24-hour Help-Line to answer Medicaid recipients' questions about participating in their health plans.

Evidence of Coverage: Any certificate, agreement, contract, or notification issued to a beneficiary that sets forth the responsibilities of the beneficiary and services available to the beneficiary.

Experimental Treatment: A course of treatment, procedure, device, or other medical intervention that is not yet recognized by the professional medical community as an effective, safe, and proven treatment for the condition for which it is being used.

External Quality Review Organization (EQRO): A requirement under Title XIX of the Social Security Act, Section 1902(a), (30), (c) for states to obtain an independent, external review body to perform an annual review of the quality of services furnished under state contracts with managed care organizations, including the evaluation of quality outcomes, timeliness, and access to services.

Family: In this document, parents, foster parents, legal guardians, or relatives who serve as a child's primary caregiver.

Family-Centered Care: Best practice principles for the provision of medical, therapeutic, and mental health care for children with special health care or developmental needs. Family-centered care establishes parents as the central members of a team of professionals that plan and implement services needed to address a child's needs; builds upon the strengths of the family; recognizes and addresses the impact of a child with special health care needs on caregivers, siblings, and other family members; and arranges for services to be provided in the home or other natural settings whenever possible.

Family Planning Services: Refer to any medically approved diagnostic procedure, treatment, counseling, drug, supply, or device which is prescribed or furnished by a provider to individuals of childbearing age for the purpose of enabling such individuals to freely determine the number and spacing of their children.

Federally Qualified Health Center (FQHC): A health center as defined in 42 CFR 405.2430 - 2470.

Federally Recognized Services: Refers to medically necessary services that must be made available to children and adolescents under the EPSDT program including the services listed in Attachment J.8.

Fee-For-Service (FFS): A payment to providers on a per-service basis for health care services.

Formulary: An exclusive list of drug products for which the contractor will provide coverage to its members, as approved by the Medicaid Program.

Fraud: The obtaining of something valuable through intentional deception or misrepresentation or concealment of the material facts. Fraud can be made by a person with the knowledge that the deception could result in some unauthorized benefit to himself/herself or another person. It includes any act that constitutes fraud under applicable Federal or state law.

General Accepted Accounting Principles (GAAP): A technical term in financial accounting. It encompasses the conventions, rules, and procedures necessary to define accepted accounting practice at a particular time. This includes not only broad guidelines of general application, but also detailed practices and procedures.

Grievance: An expression of dissatisfaction about any matter other than an action. The term is also used to refer to the overall system that includes grievances and appeals handled by the Contractor and access to the District's Fair Hearing process. (A formal Process)

Health Care Financing Administration (HCFA): A Federal agency within the U.S. Department of Health and Human Services responsible for oversight of Medicaid programs. This agency has been renamed the Center for Medicare and Medicaid Services (CMS).

Health Care Professional: A physician or any of the following: a podiatrist, optometrist, chiropractor, psychologist, dentist, physician assistant, physical or occupational therapist, therapist assistant, speech-language pathologist, audiologist, registered or practical nurse (including nurse practitioner, clinical nurse specialist, certified registered nurse anesthetist, and certified nurse midwife), license certified social worker, registered respiratory therapist, and certified respiratory therapy technician.

HealthCheck Tracking System: This universal database is a form-based process, which uses a universal encounter form. This encounter form is used by providers to simply and accurately quantifies EPSDT service information. This system works to close the gaps in EPSDT reporting as well as improve the quality of reporting.

Health Maintenance Organization (HMO): A District of Columbia licensed risk-bearing entity, which combines delivery and financing of health care and basic health services to enrolled members for a fixed, prepaid fee.

High- Risk Newborn-The term high- risk newborn can be applied to any newborn who experiences a complicated prenatal course that is at an increased risk for perinatal morbidity or mortality. Conditions affecting the high- risk newborn include severe prematurely (gestational age from 24 weeks to 32 weeks), congenital abnormalities, genetic syndromes, malignancies, acute and chronic infections, prolonged NI*CU stay* and developmental delays regardless of etiology. Maternal conditions associated with

high risk newborns include but not limited to medical or obstetrical complications, inadequate or no prenatal care, maternal age less than 18 years, mental illness, substance abuse, poor infant-maternal bonding, homelessness, poor parenting skills and a previous history of involvement with Child and Family Services.

High Cost/High-Risk Case Management: Policies and procedures for effectively managing the authorization of treatment services for beneficiaries with high cost and/or high-risk conditions to ensure efficient use of resources and high quality health outcomes.

Immediate Need: A situation in the professional judgment of the dispensing registered pharmacist, the dispensing of the drug at the time when the prescription is presented is necessary to reduce or prevent the occurrence or persistence of a serious adverse health condition.

In-Plan Services: Services that are the payment responsibility of the contractor.

Incentive Arrangement: Any payment mechanism under which a contractor shall receive additional funds over and above the capitation rates it was paid for meeting targets specified in the contract.

Income Maintenance Administration (IMA): Government of the District of Columbia agency under the Department of Human Services responsible for determining eligibility for Medicaid through TANF and TANF-related categories, and for administering determinations for SSI eligibility made by the Social Security Administration.

Individuals with Disabilities Education Act (IDEA): Federal law governing the rights of infants and toddlers to receive early intervention and children with disabilities to receive educational services.

Inquiry: Any member's request for administrative service, information, or to express an opinion. Whenever specific corrective action is requested by the member, or determined to be necessary by the contractor, it should be classified as a complaint.

Involuntary Disenrollment: The termination of membership of a beneficiary under conditions permitted in this agreement.

Joint Commission on Accreditation of Healthcare Organizations (JCAHO): National organization that sets standards for hospitals and other health care organizations and conducts reviews to determine whether they meet those standards in order to accredit them.

LaShawn Receiver: Court designated administrator of the District's Child and Family Services Agency responsible for investigating children's protective issues, exercising custodial responsibility for children who are removed from the custody of their families, and administering foster care and other services needed to care for

children while they are in the custody of the District. The role of the LaShawn Receiver has been transferred to the Child and Family Services Administration.

Limited or No English Proficiency Individual: An individual who is unable to speak, read, write, or understand the English language at a level that permits him or her to interact effectively with contractors, agencies, or providers.

Managed Care Eligibles: District of Columbia residents who have been determined eligible for Medicaid in an eligibility category that requires them to participate in Medicaid Managed Care Program by enrolling in a health plan.

Managed Care Organization (MCO): A contractor that has, or is seeking to qualify for, a comprehensive risk contract, and that is:

- A Federally qualified MCO that maintains written policies and procedures that meet the advance directives requirements of subpart I of part 489 of the CFR; or
- Any public or private contractor that meets the advance directives requirements and is determined to also meet the following conditions:
- Makes the services it provides to its Medicaid beneficiaries as accessible (in terms of timeliness, amount, duration, and scope) as those services are to other Medicaid recipients within the area served by the contractor; and
- Meets the solvency standards of CFR 438.116.

Management Information System (MIS): A computerized or other system used for collection, analysis, and reporting of information needed to support management activities.

Medicaid: A program established by Title XIX of the Social Security Act which provides payment of medical expenses for eligible persons who meet income and/or other criteria.

Medicaid Managed Care Program (MMCP): A program for the provision and management of specified Medicaid services through contracted Health Maintenance Organizations. MMCP was established pursuant to the Medicaid Managed Care Amendment Act of 1992, effective March 17, 1992 (DC Law 9-247, DC Code Section 1-3 59) as amended.

Medical Assistance Administration (MAA): The Administration within the Government of the District of Columbia, under the Department of Health responsible for administering all Medicaid services authorized by Title XIX of the Social Security Act for eligible recipients, including the Medicaid Managed Care Program and oversight of its managed care contractors.

Medical Cost: Third party claims paid for medical services covered under Medicaid, excluding those services not covered under the contract as identified in Section C.8.

Medical Necessity Criteria: Clinical determinations to establish a service or benefit that will, or is reasonably expected to:

- Prevent the onset of an illness, condition or disability;
- Reduce or ameliorate the physical, mental, behavioral, or developmental effects of an illness, condition, injury, or disability; and
- Assist the individual to achieve, maintain, or regain maximum functional capacity in performing daily activities, taking into account both the functional capacity of the individual and those functional capacities appropriate for individuals of the same age.

Medically Appropriate Transfer: A transfer from a hospital, which complies with the requirement of 42 U.S.C. §1395dd(c).

Medically Necessary Services: Services that are included in the District's Medicaid programs and meet medical necessity criteria established in the Request for Proposals.

Member Month: A beneficiary who participates in the MMCP for one month.

Member Record: A record contained on the Daily Membership File or the Monthly Membership File that contains information on eligibility, managed care coverage, and category of assistance, which serves to establish the covered services for which a beneficiary is eligible.

Mental Health and Alcohol and Drug Abuse Services: Medicaid services for the treatment of mental, emotional, and chemical dependency disorders.

National Committee on Quality Assurance (NCQA): An organization that sets standards, evaluates, and accredits health plans and other managed health care organizations.

Net Worth (Equity): The residual interest in the assets of an entity that remains after deducting its liabilities.

Network: All contracted or employed providers participating in the health care plan that provides covered services to members.

Network Provider: Health and mental health services provider who is an individual or organization selected and under contract with a specific contractor.

Non-risk Contract: A contract under which the contractor—

- Is not at financial risk for changes in utilization or for costs incurred under the contract that do not exceed the upper payment limits specified in CFR 438.116; and
- May not be reimbursed by the District at the end of the contract period on the basis of the incurred costs, subject to the specified limits.

Notice of Action: Written notice of a decision by a contractor to authorize, deny, terminate, suspend, or delay requested services for a specific beneficiary; approve or deny a grievance; approve or deny an appeal; or report on actions taken to resolve a complaint.

Ombudsman: Entity that engages in impartial and independent investigation of individual complaints, advocates on behalf of beneficiaries, and issues recommendations. This function may be operated by an organization independent of the contractor or by a designated and appropriately delineated and empowered unit in a government agency.

Open Panel: A managed care plan that contracts (either directly or indirectly) with private physicians to deliver care in their own offices. Examples would include a direct contract HMO.

Out-of-Network Provider: A health or mental health and alcohol and drug abuse individual or organization that does not have a written provider agreement with a contractor and therefore not included or identified as being the contractor's network.

Out-of-Plan Services: Services that are not included covered by the health plans.

Outreach: Activities performed by the contractor or its designee to contact its beneficiaries and their families, and to communicate information, monitor the effectiveness of care, encourage use of Medicaid resources and treatment compliance, and provide education.

Potential Beneficiary: District of Columbia residents who have been determined eligible for Medicaid in an eligibility category that requires them to participate in Medicaid Managed Care Program by enrolling in a health plan, either through mandatory enrollment or voluntarily elect to enroll, but is not yet a beneficiary of a specific MCO, CASSIP, or PCCM.

Prepaid Inpatient Health Plan (PIHP): A contractor that provides medical services to beneficiaries under contract with the District MAA, and on the basis of prepaid capitation payments, or other payment arrangements that do not use District plan payment rates; provides, arranges for, or otherwise has the responsibility for the provision of any inpatient hospital or institutional services for its beneficiaries.

Prevalent Languages: As deemed by the Mayor of the District of Columbia: Spanish, Chinese, Vietnamese, Amharic, and Braille. In addition to other languages that the District may designate when there are speakers of that language who are eligible to be served or likely to be directly affected by the contractor's program.

Primary Care: All health care services and laboratory services customarily furnished by or through a general practitioner, family physician, internal medicine physician, obstetrician/gynecologist, or pediatrician, to the extent the furnishing of those services are legally authorized in the State or District in which the practitioners' practices.

Primary Care Case Manager (PCCM): A physician, a physician group practice, an entity that employs or arranges with physicians to furnish primary care case management services or, at the District's option, any of the following:

1. physician assistant
2. nurse practitioner
3. certified nurse mid-wife

Primary Care Provider (PCP): A board-certified or board-eligible provider who has a contract with a managed care plan to provide necessary well care, diagnostic, and primary care services, and to manage covered benefits for beneficiaries in his or her caseload. A physician with a specialty of pediatrics, obstetrics/gynecology, internal medicine, family medicine, or any other specialty the contractor designates from time-to-time may serve as a PCP.

Primary Source Verification: Credentialing procedures for the review and verification of original documents submitted for credentialing, including confirmation of references, appointments, and licensure from licensing authorities. (See also "Credentialing").

Prior Authorization: A determination made by a contractor to approve or deny a provider's or beneficiary's request to provide a service or course of treatment of a specific duration and scope to a beneficiary prior to the provision of the service. (See also "Service Authorization").

Provider: An individual or organization that delivers medical, dental, rehabilitation, or mental health services.

Provider Agreement: Any MAA-approved written agreement between the contractor and a provider to provide medical or professional services to MAA beneficiaries to fulfill the requirements of the contract.

Qualified Family Planning Provider (QFPP): Any public or not-for-profit health care provider that complies with Title X guidelines/standards and receives Title X funding.

Quality Management: An ongoing, objective, and systematic process of monitoring, evaluating, and improving the quality, appropriateness, and effectiveness of care.

Recipient: A person who is Medicaid eligible to receive medical and/or behavioral health services.

Recipient Month: Any MAA beneficiary covered for one (1) month.

Rejected Claim: A claim that has erroneously been assigned a unique identifier and is removed from the claims processing system prior to adjudication.

Remittance Advice: A written explanation accompanying payment to a provider indicating how the payment is to be applied.

Residential Treatment Facility: 24-hour treatment facility primarily for children with significant behavioral problems who need long-term treatment.

Respite: A service provided in order to offer a period of relief for a family member or other non-paid caregiver of a person who has needs requiring constant monitoring, assistance with activities of daily living, and/or treatment. Respite may be provided in the home setting by alternative caretakers, or out of home in a non-acute residential, nursing, or hospital setting.

Retrospective Review: Determination of the appropriateness or necessity of services after they have been delivered, generally through the review of the medical or treatment record.

Risk Assessment: Assessment process based on medical records, phone contact, and when needed, an office visit or outreach to the home, to determine which beneficiaries are most in need of medical and related services to improve their condition.

Risk Contract: A contract under which the contractor assumes risk for the cost of the services covered under the contract and incurs loss if the cost of furnishing the services exceeds the payments under the contract.

Risk Corridor: A risk sharing mechanism in which the District and contractors share in both profits and losses under the contract outside of predetermined threshold amount, so that after an initial corridor in which the contractor is responsible for all losses or retains all profits, the State contributes a portion toward any additional losses, and receives a portion of any additional profits.

Routine: Describes a level of health needs which is neither urgent nor emergent, but for which medical services can improve functioning and/or reduce symptoms.

Salazar Monitor: Court monitor appointed to report, record, evaluate, observe, and provide recommendations to the United States District Court on the District's Medicaid program including processing of Medicaid applications and re-certification, eligibility verification, and arranging, providing, and reporting on EPSDT services.

School-Based Health Center: A school-based health care site, which provides at a minimum, age-appropriate primary and preventive health services to children in need of primary health care with the informed parental consent.

Section 1915(b) Waiver: A statutory provision of Medicaid that allows a state to partially limit the freedom of choice by beneficiaries of Medicaid eligible services or that waives the requirements under Title XIX of the Social Security Act, Medicaid Act, for statewideness of a plan or comparability of benefits.

Senior Manager: A contractor's staff member who has decision-making authority and is accountable for the performance of a major function and/or department.

Service Authorization Request: A managed care beneficiary's request for the provision of a service.

Sixth Omnibus Budget Reconciliation Act (SOBRA): A Federal statute that allows states to expand coverage to pregnant women and children.

Special Health Care Needs: See Adult or Children with Special Health Care Needs.

Spend-down: A process of establishing eligibility by allowing beneficiaries to spend their excess net income on certain incurred or paid medical expenses. Eligibility may need to be redetermined monthly.

Stabilize: The provision of treatment necessary to assure, within reasonable medical probability, that no material deterioration of a beneficiary's medical condition is likely to result.

Start Date: The first date in which beneficiaries are eligible for medical services under the operational contract and on which the contractors are operationally responsible and financially liable for providing medically necessary services to beneficiaries.

State Children's Health Insurance Program (SCHIP): Passed as part of the Balanced Budget Act of 1997, the Children's Health Insurance Program provides health insurance for children who come from working families with incomes too high to qualify for Medicaid, but too low to afford private health insurance.

Subcapitation: A provider in the contractor's network paid on a per member/per month basis to cover some or all of its services. This method passes on a portion of risk to providers. (For more detail, see Risk Contract).

Subcontract: Any written agreement between the contractor and another party that requires the other party to provide services or benefits that the contractor shall make available.

Supplemental Security Income (SSI): A Medicaid category of assistance for blind or disabled individuals who are eligible for Federal Supplemental Security Income benefits and Medicaid.

SSI-Related: A Medicaid category, which includes, but is not limited to the same requirements as the corresponding category of SSI. Persons who receive Medicaid in SSI-Related categories may include, but are not limited to the aged, blind, or disabled and people determined to be Medically Needy.

Sui Juris: Having full legal rights or capacity as in the case of emancipated minors.

Temporary Assistance for Needy Families (TANF): Federally funded program that provides assistance to single parent families with children who meet the categorical requirements for aid. TANF eligibles also qualify for Medicaid coverage.

TANF-related Individuals: Persons who qualify for Medicaid and whose family incomes do not exceed 200% of FPL. TANF-related eligibility is determined by the District's State Medicaid Plan or Federal law (including medically needy and transitional Medicaid).

The Rehabilitation Accreditation Commission (CARF): An international accreditation organization that develops and maintains practical and relevant standards of quality for programs and services, formerly known as the Commission Accreditation of Rehabilitation Facilities**. (CARF maintained its acronym).**

Third Party Liability: An insurance policy or other form of coverage whose responsibility it is to pay for certain health services for a Medicaid eligible person. Includes commercial health insurance, worker's compensation, casualty, torts, and estates. These sources shall be used to offset the costs of Medicaid services.

Third Party Resource (TPR): A third party resource is any individual, entity or program that is liable to pay all or part of the medical cost of injury, disease, or disability of a beneficiary. Examples of third party resources would include government insurance programs such as Medicare or CHAMPUS (Civilian Health and Medical Program of the Uniformed Services); private health insurance companies or carriers; liability or casualty insurance; and court-ordered medical

support. Such resources, or insurance, shall be billed prior to billing the Medicaid Program, but a TPR should never interfere with a Medicaid beneficiary's receipt of service.

Timeliness of Oral Interpretive Services as defined by category:

Emergency Services –The contractor shall ensure that all providers of emergency services furnish or arrange for oral interpreter services on a 24 hour, 7 day a week basis immediately after a request for such services by a beneficiary or on behalf of a beneficiary with limited English proficiency; or a determination by the treating provider that the beneficiary requires such services.

Non-Emergency Services –The contractor shall furnish, or arrange for the furnishing of oral interpreter services to the beneficiary with limited English proficiency; at the time a scheduled appointment begins or within one (1) hour of the time an unscheduled appointment is requested by or on behalf of the beneficiary with limited English proficiency.

Timely: Filing on or before the later of the following: within sixty (60) days of the contractor's mailing the notice of action and the intended effective date of the contractor's proposed action.

Title XVIII (Medicare): A Federally-financed health insurance program administered by the Centers for Medicaid and Medicare Services (CMS), covering almost all Americans sixty-five (65) years old and older and certain individuals under sixty-five (65) who are disabled or have chronic kidney disease. The program provides protection with an acute care focus under two parts: (I) Part A covers inpatient hospital services, post-hospital care in skilled nursing facilities and care in patients' homes; and (2) Part B covers primarily physician and other outpatient services.

Transportation Services: Mode of transportation that can suitably meet Beneficiary's medical needs. Acceptable forms of providing transportation include, but are not limited to, provision of bus, subway, or taxi vouchers, wheel chair vans, and ambulances.

Triage: The process of determining the degree of urgency of the needs of an individual beneficiary, and then referring and/or further arranging for that individual beneficiary to receive appropriate services.

TTD/TTY: A telecommunications instrument enabling those with communication disorders to communicate over the telephone by using a keyboard. Also known as Teletype (TTY) or TTD.

Urban: Consists of territory, persons, and housing units in places, which are designated as 2,501 persons or more. These places shall be in close proximity to one another.

Urgent Medical Condition: A condition, including a mental health and/or alcohol and drug abuse condition, less serious than an emergency medical condition, which is severe and/or painful enough to cause a prudent layperson, possessing an average knowledge of medicine, to believe that his or her condition requires medical evaluation or treatment within 24 hours in order to prevent serious deterioration of the individual's condition or health.

Utilization Management: An objective and systematic process for planning, organizing, directing, and coordinating health care resources to provide medically necessary, timely, and quality health care services in the most cost-effective manner.

Utilization Review Criteria: Detailed standards, guidelines, decision algorithms, models, or informational tools that describe the clinical factors to be considered relevant to making determinations of medical necessity including, but not limited to, level of care, place of service, scope of service, and duration of service.

Vital Documents: Notices, complaint/appeal forms, enrollment and outreach materials that inform individuals about their rights and/or eligibility requirements for benefits and participation under the District's services, programs, and activities.

Waiver: A process by which a state may obtain an approval from CMS for an exception to a Federal Medicaid requirement(s).

Waste: The incurring of unnecessary cost as a result of deficient practices, systems, or control.

Youth Services Administration (YSA): Government of the District of Columbia agency under the Department of Health and Human Services responsible for administering services for youth who are in the custody of the District as a result of criminal activities.

Acronyms

ADA	Americans with Disabilities Act
AMBHA	American Managed Behavioral Healthcare Association
APRA	Addictions, Prevention, Recovery Administration
CAHPS	Beneficiary Assessment of Health Plans Studies
CARF	The Rehabilitation Accreditation Commission, formerly known as the Commission Accreditation of Rehabilitation Facilities. (CARF changed its name but maintained its acronyms.)
CAP	Corrective Action Plan
CASSIP	Child and Adolescent SSI or 551-Related Plans
CLIA	Clinical Laboratory Improvement Amendment
CMHS	Commission on Mental Health Services
CMS	Center for Medicare and Medicaid Services
CO	Contracting Officer
CTR	Contracting Officer Technical Representative
CQI	Continuous Quality Improvement
CSFP	Commodities Supplemental Food Program
DBE	Disadvantaged Business Enterprise
DCHFP	District of Columbia Healthy Families Program
DCPS	District of Columbia Public Schools
DME	Durable Medical Equipment
DCES	District of Columbia Department of Employment Services
DOH	Department of Health
D-U-N-S	Data-Universal-Numbering-System
DUR	Drug Utilization Review
EOB	Explanation of Benefits
EPSDT	Early and Periodic Screening, Diagnosis, and Treatment
EQRO	External Quality Review Organization
ESA	Employment Standards Administration
EVS	Eligibility Verification System
FFS	Fee-For-Service
FPL	Federal Poverty Level
FQHC	Federally Qualified Health Center
FTE	Full Time Equivalent Employees
HCFA	Health Care Finance Administration, now called the Center for Medicare and Medicaid Services (CMS).
HEDIS	Health Plan and Employer Data and Information Set
HIPAA	Health Insurance Portability and Accountability Act
HMO	Health Maintenance Organization
ICF/MR	Intermediate Care Facilities for Mental Retardation
IDEA	Individuals with Disabilities Education Act
IDIQ	Indefinite Delivery Indefinite Quantity
IEP	Individualized Education Plan
IFB	Invitation for Offers

IFSP	Individualized Family Services Plan
IMA	Income Maintenance Administration
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
LBE	Local Business Enterprise
LBOC	Local Business Opportunity Commission
LEP	Limited or No English Proficiency
MAA	Medical Assistance Administration
MH	Mental Health
MIS	Management Information System
MMCP	Medicaid Managed Care Program
MOU	Memorandum of Understanding
NAIC	National Association of Insurance Commissioners
NCQA	National Committee on Quality Assurance
OHRLBD	Office of Human Rights and Local Business Development
OIG	Office of Inspector General, U.S. Department of Health and Human Services
OMB	Federal Office of Managed Budget
OMC	Office of Managed Care
OPI	Office of Program Integrity
OTMP	Outreach and Transition Monitoring Plan
PBM	Pharmacy Benefits Manager
PCP	Primary Care Physician
PMPM	Per Member Per Month
QFPP	Qualified Family Planning Provider
QA	Quality Assessment
QI	Quality Improvement
QISMC	Quality Improvement System for Managed Care
RFP	Request for Proposal
SA	Substance Abuse
SCHIP	State Children's Health Insurance Program
SOBRA	Sixth Omnibus Budget Reconciliation Act
SSI	Supplemental Security Income
TANF	Temporary Assistance to Needy Families
TDL	Technical Direction Letter
TPL	Third Party Liability
TTY	Teletype
UPL	Upper Payment Limit
URAC	Utilization Review Accreditation Commission
VFC	Vaccines for Children

WIC	Women, Infants and Children
YSA	Youth Services Administration

"THE LIVING WAGE ACT OF 2006"

Title I, D.C. Law No. 16-118, (D.C. Official Code §§ 2-220.01-.11)

Effective June 9, 2006, recipients of new contracts or government assistance shall pay affiliated employees and subcontractors who perform services under the contracts no less than the current living wage $11.75 per hour.

The requirement to pay a living wage applies to:

- All recipients of contracts in the amount of $100,000 or more; and, all subcontractors of these recipients receiving $15,000 or more from the funds received by the recipient from the District of Columbia, and,
- All recipients of government assistance in the amount of $100,000 or more; and, all subcontractors of these recipients of government assistance receiving $50,000 or more in funds from government assistance received from the District of Columbia.

"Contract" means a written agreement between a recipient and the District government.
"Government assistance" means a grant, loan or tax increment financing that result in a financial benefit from an agency, commission, instrumentality, or other entity of the District government.
"Affiliated employee" means any individual employed by a recipient who received compensation directly from government assistance or a contract with the District of Columbia government, including any employee of a contractor or subcontractor of a recipient who performs services pursuant to government assistance or contract. The term "affiliated employee" does not include those individuals who perform only intermittent or incidental services with respect to the contract or government assistance or who are otherwise employed by the contractor, recipient or subcontractor.

Certain exceptions may apply where contracts or agreements are subject to wage determinations required by federal law which are higher than the wage required by this Act; contracts for electricity, telephone, water, sewer other services delivered by regulated utility; contracts for services needed immediately to prevent or respond to a disaster or eminent threat to the public health or safety declared by the Mayor; contracts awarded to recipients that provide trainees with additional services provided the trainee does not replace employees; tenants or retail establishments that occupy property constructed or improved by government assistance, provided there is no receipt of direct District government assistance; Medicaid provider agreements for direct care services to Medicaid recipients, provided that the direct care service is not provided through a home care agency, a community residential facility or a group home for mentally retarded persons; and contracts or other agreements between managed care organizations and the Health Care Safety Net Administration or the Medicaid Assistance Administration to provide health services.

Exemptions are provided for employees under 22 years of age employed during a school vacation period, or enrolled as a full-time student who works less than 25 hours per week, provided that other employees are not replaced, and for employees of nonprofit organizations that employ not more than 50 individuals.

Each recipient and subcontractor of a recipient shall provide this notice to each affiliate employee covered by this notice, and shall also post this notice concerning these requirements in a conspicuous site in the place of business.

All recipients and subcontractors shall retain payroll records created and maintained in the regular course of business under District of Columbia law for a period of at least 3 years.

This is a summary of the "Living Wage Act of 2006". For the complete text go to:
www.does.dc.gov *or* www.ocp.dc.gov

To file a complaint contact: **Department of Employment Services**
Office of Wage-Hour
64 New York Avenue, N.E., Room 3105, Washington, D.C. 20002
(202) 671-1880

LIVING WAGE ACT FACT SHEET

The "Living Wage Act of 2006," Title I of D.C. Law 16-18, (D.C. Official Code §§2-220.01-.11 became effective June 9, 2006. It generally provides that District of Columbia government contractors and recipients of government assistance (grants, loans, tax increment financing) in the amount of $100,000 or more shall pay affiliated employees wages no less than the amount of $11.75 per hour.

Subcontractors of D.C. government contractors who receive $15,000 or more from the contract and subcontractors of the recipients of government assistance who receive $50,000 or more from the assistance are also required to pay their affiliated employees no less than $11.75 per hour.

"Affiliated employee" means any individual employed by a recipient who received compensation directly from government assistance or a contract with the District of Columbia government, including any employee of a contractor or subcontractor of a recipient who performs services pursuant to government assistance or contract. The term "affiliated employee" does not include those individuals who perform only intermittent or incidental services with respect to the contract or government assistance or who are otherwise employed by the contractor, recipient or subcontractor.

Exemptions – The following contracts and agreements are exempt from the ***"Living Wage Act"***:

1. Contracts or other agreements that are subject to higher wage level determinations required by federal law (i.e., if a contract is subject to the Service Contract Act and certain wage rates are lower than the District's current living wage, the contractor must pay the higher of the two rates);

2. Existing and future collective bargaining agreements, provided, that the future collective bargaining agreement results in the employee being paid no less than the established living wage;

3. Contracts for electricity, telephone, water, sewer or other services provided by a regulated utility;

4. Contracts for services needed immediately to prevent or respond to a disaster or eminent threat to public health or safety declared by the Mayor;

5. Contracts or other agreements that provide trainees with additional services including, but not limited to, case management and job readiness services; provided that the trainees do not replace employees subject to the Living Wage Act of 2006;

6. An employee, under 22 years of age, employed during a school vacation period, or enrolled as a full-time student, as defined by the respective institution, who is in high school or at an accredited institution of higher education and who works less than 25 hours per week; provided that he or she does not replace employees subject to the Living Wage Act of 2006;

7. Tenants or retail establishments that occupy property constructed or improved by receipt of government assistance from the District of Columbia; provided, that the tenant or retail establishment did not receive direct government assistance from the District;

8. Employees of nonprofit organizations that employ not more than 50 individuals and qualify for taxation exemption pursuant to section 501(c)(3) of the Internal Revenue Code of 1954, approved August 16, 1954 (68A Stat. 163; 26 U.S.C. § 501(c)(3);

9. Medicaid provider agreements for direct care services to Medicaid recipients, provided, that the direct care service is not provided through a home care agency, a community residence facility, or a group home for mentally retarded persons as those terms are defined in section 2 of the Health-Care and Community Residence Facility, Hospice, and Home Care Licensure Act of 1983, effective February 24, 1984 (D.C. Law 5-48; D.C. Official Code § 44-501); and

10. Contracts or other agreements between managed care organizations and the Health Care Safety Net Administration or the Medicaid Assistance Administration to provide health services.

Enforcement

The Department of Employment Services (DOES) and the D.C. Office of Contracting and Procurement (OCP) share monitoring responsibilities.

If you learn that a contractor is not paying at least the living wage you should report it to the Contracting Officer.

If you believe that your employer is not paying you at least the required living wage, you may file a complaint with the DOES Office of Wage – Hour, located at 64 New York Avenue, N.E., Room 3105, (202) 671-1880.

For questions and additional information, contact the Office of Contracting and Procurement at (202) 727-0252 or the Department of Employment Services on (202) 671-1880.

Please note: *This fact sheet is for informational purposes only as required by Section 106 of the Living Wage Act. It should not be relied on as a definitive statement of the Living Wage Law or any regulations adopted pursuant to the law.*

Government of the District of Columbia
Anthony A. Williams, Mayor

Department of Employment Services
Gregory P. Irish, Director

DRUG-FREE WORKPLACE CERTIFICATION

1. CERTIFICATION REGARDING A DRUG-FREE WORKPLACE (JULY - 1990):

1.1 Definitions. As used in this provision:

1.1.1 **Controlled substance**: means a controlled substance in schedules I through V of Section 202 of the Controlled Substances Act (21 U.S.C. 812) and as further defined in regulation at 21 CFR 1308.11 - 1308.15.

1.1.2 **Conviction:** means a finding of guilt (including a plea of nolo contendere) or imposition of sentence, or both, by any judicial body charged with the responsibility to determine violations of the Federal or State criminal drug statutes.

1.1.3 **Criminal drug statute:** means a Federal or non-Federal criminal statute involving the manufacture, distribution, dispensing, possession or use of any controlled substance.

1.1.4 **Drug-free workplace:** means the site(s) for the performance of work done by the Contractor in connection with a specific contract at which employees of the Contractor are prohibited from engaging in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance.

1.1.5 **Employee:** means an employee of a Contractor directly engaged in the performance of work under a Government contract. "Directly engaged" is defined to include all direct cost employees and any other Contractor employee who has other than a minimal impact or involvement in contract performance.

1.1.6 **Individual:** means an Offeror/Contractor that has no more than one employee including the Offeror/Contractor.

1.2 By submission of its offer, the Offeror, if other than an individual, who is making an offer that equals or exceeds $25,000, certifies and agrees, that with respect to all employees of the Offeror to be employed under a contract resulting from this solicitation, it will - no later than 30 calendar days after contract award (unless a longer period is agreed to in writing), for contracts of 30 calendar days or more performance duration: or as soon as possible for contracts of less than 30 calendar days performance duration, but in any case, by a date prior to when performance is expected to be completed:

1.2.1 Publish a statement notifying such employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the Contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition;

1.2.2 Establish an ongoing drug-free awareness program to inform such employees about the following:

(i) The dangers of drug abuse in the workplace;

(ii) The Contractor's policy of maintaining a drug-free workplace;

(iii) Any available drug counseling, rehabilitation, and employee assistance programs; and

(iv) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace.

1.2.3 Provide all employees engaged in performance of the contract with a copy of the statement required by subparagraph 1.2.1 of this provision;

1.2.4 Notify such employees in writing in the statement required by subparagraph 1.2.1 of this provision that, as a condition of continued employment on the contract resulting from this solicitation, the employee will:

(i) Abide by the terms of the statement; and

(ii) Notify the employer in writing of the employee's conviction under a criminal drug statute for a violation occurring in the workplace no later than 5 calendar days after such conviction;

1.2.5 Notify the Contracting Officer in writing within 10 calendar days after receiving notice under subdivision 1.2.4 (ii) of this provision, from an employee or otherwise receiving actual notice of such conviction. The notice shall include the position title of the employee; and

1.2.6 Within 30 calendar days after receiving notice under subdivision 1.2.4 (ii) of this provision of a conviction, takes one of the

following actions with respect to any employee who is convicted of a drug abuse violation occurring in the workplace:

(i) Take appropriate personnel action against such employee, up to and including termination; or

(ii) Require such employee to satisfactorily participate in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency.

1.2.7 Make a good faith effort to maintain a drug-free workplace through implementation of subparagraphs 1.2.1 through 1.2.6 of this provision.

1.3 By submission of its offer, the Offeror, if an individual who is making an offer of any dollar value, certifies and agrees that the Offeror will not engage in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance in the performance of the contract resulting from this solicitation.

1.4 Failure of the Offeror to provide the certification required by paragraphs 1.2 through 1.3 of this provision, renders the Offeror unqualified and ineligible for award.

1.5 In addition to other remedies available to the Government, the certification in paragraphs 1.2 through 1.3 of this provision concerns a matter within the jurisdiction of an agency of the United States and the making of a false, fictitious, or fraudulent certification may render the maker subject to prosecution under Title 18, United States Code, Section 1001.

1.6 CERTIFICATION REGARDING A DRUG-FREE WORKPLACE

_____ _____

AUTHORIZED CONTRACTOR PERSONNEL (PRINT NAME) TITLE

_____ _____

Signature of Authorized Contractor Personnel Date