DISTRICT OF COLUMBIA
DEPARTMENT OF CORRECTIONS

PROGRAM MANUAL

OPI: OGC
Number: 1300.3
Date: December 15, 2003
Subject: Health Information Privacy

1. **PURPOSE AND SCOPE.** To provide uniform guidelines for implementation of DC Privacy Rules for Protected Health Information.

2. **POLICY.** It is the policy of the DC Department of Corrections (DOC) to implement and enforce policies and procedures that fulfill its legal obligations required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA regulations seek to protect the health information of individuals; and give individuals certain rights regarding their health information while also seeking to meet the needs of the health care industry to more efficiently process health-care claims and certain other related transactions. DOC provides guidelines herein to ensure sound and appropriate administrative, physical, and technical safeguards against any reasonably anticipated unauthorized use or disclosure, or any reasonably anticipated threat or hazard to the privacy, security or integrity of protected health information (PHI).

3. **APPLICABILITY**

   a. **Covered Entities.** Under HIPAA Privacy Rules, the District Government, designated DC agencies and designated business associates are covered entities. This policy shall apply to DOC employees and affected DOC business associates and their employees who use and disclose protected health information about inmates who are in the custody of the DOC. The primary covered entities are:

      1) DC Department of Corrections (DOC).

      2) The health care provider which is the Center for Correctional Health and Policy Studies (CCHPS).

      3) The Corrections Corporation of America Correctional Treatment Facility (CCA/CTF).

      4) The food services provider (ARAMARK).

      5) Community Correctional Residential Programs (CCRP) that contract with DOC.

6) Others that are in relationship with DOC to provide health related treatment/services (area hospitals, etc.).

b. **Records of Former Inmates.** For the purposes of this provision, once the inmate is released on parole, probation, supervised release, or is otherwise no longer in lawful custody, this individual may request copies of his/her PHI. The PHI shall be subject to HIPPA Privacy Rules as authorized in CFR 164.512(k)(5)(iii).

c. **Designated Record Sets.** For the purpose of this directive, the term *record* means any item, collection or grouping of information that includes or contains data that identifies protected health information (PHI) and is maintained, collected, used or disseminated by or for a covered entity. In this sense all records, within the DOC and its business associates, containing data that identifies patient health information shall be considered part of the *Designated Record Set* (see Chapter 3 for further details).

4. EXCLUSIONS

a. **Employment Records.** Health information in employment records held by DOC in its role as employer is exempt from the definition of PHI. DOC and its covered health care business associates shall continue to use and disclose DOC employee records in accordance with DPM Chapter 31A "Records Management and Privacy of Records" and other applicable regulations, policy and procedure.

b. **Educational Records.** Educational records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g.

c. **Security Restrictions for Inmate Access.** Inmates shall be given the opportunity to inspect their PHI provided it is not determined to jeopardize their safety, the safety of other inmates or staff as further outlined in Section 5 below and in Chapter 2 of this directive.

d. **Copy Restrictions for Inmates.** Inmates shall not be given a copy of their protected health information because to do so would not ensure appropriate physical safeguards of the documents and may further jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of any officer, employee or other person at the correctional institution or responsible for transporting the inmate.

e. **Privacy Practices Notice.** Individual Privacy notices shall not be issued to inmates who are confined to a correctional institution that is a covered entity (45 CFR 164.520 (a)(3). Protection, use and disclosure of PHI about inmates are set forth in this directive.

f. **Psychotherapy Notes.** Personal notes shall never be disclosed to anyone, with or without authorization, except in litigation brought by the individual against the mental health professional alleging malpractice or wrongful disclosure of mental health information. As a precaution, psychotherapy notes and personal notes must be maintained separately from an individual's official record of mental health information so as to avoid their incidental disclosure in connection with an otherwise valid disclosure of the record.

5. **USE AND DISCLOSURE**

a. Under HIPAA Privacy Rules, DOC and its health care business associates shall use and disclose protected health information (PHI) about inmates without the inmate's permission as outlined in Chapter 5 of this directive.

b. Inmates in the custody of the DOC or a DOC contract facility shall be granted the opportunity to inspect their individual PHI. Certain PHI, subject to rules listed in this directive in Chapter 7, Section 2 §§c and e, shall be removed from the medical record prior to the inmate's inspection.

6. **NOTICE OF NON-DISCRIMINATION.**

a. In accordance with the D.C. Human Rights Act of 1977, as amended, D.C. Code section 2.1401.01 et seq., (Act) the District of Columbia does not discriminate on the basis of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, familial status, family responsibilities, matriculation, political affiliation, disability, source of income, or place of residence or business. Sexual harassment is a form of sex discrimination which is also prohibited by the Act. Discrimination in violation of the Act will not be tolerated. Violators will be subject to disciplinary action.

b. DOC prohibits discrimination against inmates when making administrative decisions and in providing access to programs.

7. DIRECTIVES AFFECTED

a. Directives Rescinded

1) PS 6300.3 "Medical Records" (5/30/00)

b. Directives Referenced

1) PS 1300.1B "District of Columbia Freedom of Information Act (FOIA)" (12/15/03)

2) PS 1300.2A "Consent to Release of Information" (12/15/03)

3) 1300.3TRM "Health Privacy Information Operations" (1/12/04)

4) PS 1311.1C "Management Controls – Research Activity" (5/20/02)

5) DO 1320.1A "Inquiries and Request from Governmental Officials and Agencies" (8/31/90)

6) PS 2000.2 "Retention and Disposal of Department Records" (4/6/01)

7) PS 2420.4A "E-Mail and Internet Usage" (9/30/03)

8) PS 2420.2 "Information Security" (12/15/03)

9) PS 2420.8 "Disaster Recovery Plan" (12/15/03)

10) PS 2921.2 "Reporting on the Job Injuries" (6/25/82)

11) DO 3800.2 "Section 504 Handicapped Americans with Disability Act Accommodations" (8/10/92)

12) PS 3800.3 "ADA: Communications for Deaf and Hearing Impaired" (9/30/03)

13) PS 4060.2A "Inmate Record" (2/15/00)

14) DO 4160.3C "Attorney-Client Relationship" (2/28/79)

15) PS 4740.1C "Culinary Workers-Examination and Daily Workers Inspection" (1/12/01)

16) PS 6000.1 "Medical Management" (12/15/03)

c. **Health Care Provider (CCHPS) Policies and Procedures**

1) 800.0 "Medical Record Confidentiality" (4/12/03)

2) 801.0 "Medical Record Format And Content" (4/12/03)

3) 802.0 "Sharing of Health Information" (4/12/03)

4) 803.0 "Availability and Use of Medical Records" (4/12/03)

5) 900.0 "Informed Consent" (4/12/03)

8. **OBJECTIVES**

a. Protected health information shall be used, stored and disclosed in accordance with HIPAA Privacy Rules as implemented in this directive.

b. All employees shall receive appropriate training in what constitutes protected health information and guidance to ensure appropriate use and disclosure.

c. Each designated record set that is maintained shall be identified and the titles of persons or offices responsible for receiving and processing access requests shall be identified. Documentation shall be maintained on *DOC – HIPAA FORM 5—DOC Designated Record Set Determinations* (Attachment A).

9. **AUTHORITY**

a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) DC Privacy Rules

b. 45 Code Federal Regulations Parts 160 and 164 (Privacy Rules)

c. 42 USCS §263a Certification Of Laboratories

d. 5 USCS §552a Public Information; agency rules, opinions, orders, records, and proceedings

e. The Computer Security Act of 1987, Public Law 100-235 (January 8, 1988)

f. D.C. Code Section 2-531 et seq.

g. Title 7 Human Health Care and Safety, Chapter 12 Mental Health Information, §7-1201.3 and §7-1202.06

h. D.C. Code § 24-211.02 Powers; Promulgation of Rules [Formerly § 24-442]

i. District Personnel Regulations Chapter 31A "Records Management and Privacy of Records"

j. HIPAA DC Guide on Preparing Contingency Plans, HIPAA DC Program Management Enterprise Compliance Implementation Project (June 2003)

k. Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g

10. **STANDARDS**

a. American Correctional Association (ACA) 3rd Edition, Standards For Adult Local Detention Facilities: 3-ALDF-4E-22, 3-ALDF-4E-42, 3-ALDF-4E-43, 3-ALDF-4E-44, 3-ALDF-4E-45, 3-ALDF-4E-46, 3-ALDF-4E-47 and 3-ALDF-4E-48

b. American Correctional Association (ACA) 4th Edition, Standards for Adult Correctional Institutions: 4-4354, 4-4396, 4-4397, 4-4402, 4-4410, 4-4413, 4-4414 and 4-4415

c. National Commission on Correctional Health Care 1997: P-09, P-11, P-12, P-42, P-53, P-57, P-60 through P-65, P-67, P-68, P-70, P-71 and P-72

Odie Washington
Director

Table of Contents

	Purpose and Scope	Page 1
	Policy	Page 1
	Applicability	Page 1
	Exclusions	Page 2
	Use and Disclosure	Page 3
	Notice of Non-Discrimination	Page 3
	Directives Affected	Page 3
	Objectives	Page 5
	Authority	Page 5
	Standards	Page 6
	Table of Contents	Page 7
Chapter 1	Introduction	Page 13
Chapter 2	General Requirements	Page 14
	District of Columbia Privacy Official	Page 14
	Training	Page 14
	HIPAA Project Manager	Page 14
	Internal Controls, Compliance and Accreditation	Page 15
	DOC Privacy Officer	Page 15
	Contracts	Page 16
	DOC Business Associates	Page 16
	Employee Responsibilities	Page 16

Chapter 3	Protected Health Information (PHI)	Page 19
	PHI in Medical Records	Page 19
	PHI in Official Inmate Institutional Files	Page 19
	Medical Designated Record Set – Common Types of PHI in	Page 20
	Non-medical Designated Record Set – Common Types of PHI in	Page 21
Chapter 4	Security for Protected Health Information	Page 22
	Information Security	Page 22
	Disaster Recovery Plan	Page 22
	General Requirements	Page 23
	Incidental Use and Disclosure	Page 23
	Verbal Communications	Page 23
	Custody and Storage	Page 23
	Telephone	Page 24
	Faxing	Page 24
	Copying	Page 25
	E-mail	Page 25
	Personnel Changes	Page 25
Chapter 5	Permitted Uses and Disclosures	Page 27
	Terms – Meaning/applications of Use and Disclosure	Page 27
	Permitted Use/Disclosures w/o Inmate Authorization	Page 28
Chapter 6	Exceptions to Permitted Disclosure – Denial of Access	Page 34
Chapter 7	Inmate Request for Access to PHI	Page 35
	Translator Services	Page 35

	Inmate Access to PHI in Their Medical Records	Page 35
	Risk of Harm if PHI is Disclosed	Page 36
	Inmate Supervision During Records Review	Page 36
	Inmate Access to PHI in Institutional File	Page 36
Chapter 8	Procedures for Disclosure of PHI	Page 38
	Review of Request for Access to PHI (DOC –HIPAA Form 38A)	Page 38
	Inmate Consent to Release PHI (DOC-HIPAA Form 3)	Page 38
	PHI Access-Personal Representative' (DOC-HIPAA Form 38A)	Page 39
	Revocation of Consent (DOC-HIPAA Form 3)	Page 39
	Verification of Identity (DOC-HIPAA Form 10)	Page 39
	Evidence of Authority to Access PHI (DOC-HIPAA Form 10)	Page 40
	Minimum Necessary Rules (DOC-HIPAA Form 10)	Page 41
	Restrictions to PHI Disclosure for Law Enforcement Purposes	Page 42
	Disclosure of Entire Medical Record – 3rd Party Request	Page 42
	Referral of Non-routine Requests for PHI to DOC Privacy Officer	Page 43
	Granting Access to Records (DOC-HIPAA Form 38D)	Page 43
	Denial of Access to PHI (DOC-HIPAA Form 38E)	Page 43
	Right of Review to Denial of Access to PHI	Page 44
	Access Fees	Page 45
	Research Studies (DOC-HIPAA Form 12)	Page 45
Chapter 9	Disclosure Accounting	Page 47
	Form 10 and ePartners Automated Accounting/Tracking	Page 47

	PHI Types - Disclosure that must be accounted for	Page 48
	Request for Disclosure Accounting (DOC-HIPAA Form 40A)	Page 49
Chapter 10	Request to Amend, Restrict Disclosure and Complaints	Page 50
	Request to Amend PHI (DOC-HIPAA Form 39A)	Page 50
	Granting the Amendment (DOC-HIPAA Form 39C)	Page 51
	Denying the Amendment (DOC-HIPAA Form 39E)	Page 51
	Request to Restrict Use/Disclosure (DOC-HIPAA Form 42A)	Page 52
	Unenforcable Restrictions and Use in Medical Emergencies	Page 53
	DOC Agreement to Restrict Disclosure (DOC-HIPAA Form 42B)	Page 53
	Termination-Disclosure Restriction (DOC-HIPAA Forms 43A/B)	Page 54
	Denial of Restriction for Disclosure (DOC-HIPAA Forms 42E)	Page 54
	Request for Confidential Communications	Page 55
	Complaint Procedures (DOC-HIPAA Forms 53A/53B/53C)	Page 55
Chapter 11	Records Maintenance, Retention and Disposal	Page 56
	ePartner	Page 56
	Records Retention and Disposal	Page 56
	Policy and Procedures Change Documentation	Page 57
	Retention of Disclosure Documentation	Page 57
Chapter 12	Oversight and Quality Assurance	Page 58
	Contract Administration and Quality Assurance	Page 58
	Department of Health and Human Services Enforcement	Page 58
Chapter 13	Definitions	Page 61

Appendix Attachments

Attachment #	Form #	Form Name
A-1	DOC-HIPAA FORM 5	Medical Designated Record Set
A-2	DOC-HIPAA FORM 5	Institutional File - Designated Record Set
B	DOC-HIPAA FORM 38A	Request to Access PHI
C	DOC-HIPAA FORM 10	Disclosure Log/Authority Verification/ Minimum Necessary Requirement
D	DOC-HIPAA FORM 3	Consent to Release PHI
E	DOC-HIPAA FORM 38B	Direction to Retrieve Records
F	DOC-HIPAA FORM 38C	PHI Access Request Processing
G	DOC-HIPAA FORM 38D	Grant of Access to Records
H	DOC-HIPAA FORM 38E	Denial of Access to Records
I	DOC-HIPAA FORM 12	Research Access Request
J	DOC-HIPAA FORM 40A	Request for Accounting of PHI Disclosure
K	DOC-HIPAA FORM 40B	Disclosure Accounting
L	DOC-HIPAA FORM 39A	Request to Amend PHI
M	DOC-HIPAA FORM 39B	Amendment Request Processing
N	DOC-HIPAA FORM 39C	Grant of Amendment to Records
O	DOC-HIPAA FORM 39D	Notification to Amend Records
P	DOC-HIPAA FORM 39E	Denial of Amendment of Records
Q	DOC-HIPAA FORM 42A	Request to Restrict Disclosure of PHI
R	DOC-HIPAA FORM 42B	Agreement to Restrict Disclosure of PHI

Attachment #	Form #	Form Name
S	DOC-HIPAA FORM 42C	Notification-Restriction on PHI Disclosure
T	DOC-HIPAA FORM 42D	Processing for Request to Restrict
U	DOC-HIPAA FORM 43A	Notice of Termination of PHI Restriction
V	DOC-HIPAA FORM 43B	Notice to Business Assoc – Termination
W	DOC-HIPAA FORM 42E	Denial of Request to Restrict Disclosure
X	DOC-HIPAA FORM 53A	Complaint
Y	DOC-HIPAA FORM 53B	Complaint Investigation and Processing
Z	DOC-HIPAA FORM 53C	Report on Complaint

CHAPTER 1

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) originated as federal legislation and was passed in 1996. This act established standards for the protection, privacy, security and release of health information about individuals. Compliance with the privacy regulations became affective April 14, 2003.

HIPAA legislation mandated regulations that provide standards for the electronic transmission of PHI transactions, protect the privacy and security of an inmate's PHI, offer inmates specific rights regarding their PHI and establish guidelines that enable the health care industry to process claims and transactions more efficiently.

DOC is a covered entity that contracts health care services for DOC inmates through The Center For Correctional Health and Policy Studies (CCHPS). CCHPS is therefore a DOC business associate and thus is a covered entity. ARAMARK (food service provider) and Community Corrections Residential Programs (CCRP), under contract to DOC are also business associates who are covered entities.

Under HIPAA Privacy Rules, DOC, CCHPS, CCA/CTF, ARAMARK and CCRP shall respectively ensure that there are appropriate administrative, technical and physical safeguards to protect the privacy of protected health information about inmates and employees. DOC, CCHPS, CCA/CTF, ARAMARK and CCRP shall comply with applicable requirements under HIPAA Privacy Rules and shall preserve the right to maintain their current policies, procedures, and practices relating to the protected health information when these policies, procedures, and practices are more stringent than HIPAA.

Only designated employees with particular job functions are authorized to **Use** and **Disclose** protected health information. Each member of the District's workforce, shall be responsible for learning and understanding the parts of the rule that generally govern the agency; and where applicable, specifically affects their compliance during daily performance of their individual duties.

CHAPTER 2

REQUIREMENTS – GENERAL

1. **DISTRICT OF COLUMBIA PRIVACY OFFICIAL.** HIPAA shall be administered under the District of Columbia Office of Healthcare Privacy and Confidentiality.

   a. The **District of Columbia Government Privacy Official** can be contacted at:

      Privacy Official
      Office of the Deputy Mayor for Children, Youth, Families and Elders
      1350 Pennsylvania Avenue NW, Suite 307
      Washington, DC 20004
      Telephone: (202) 727-8001 Fax: (202) 727-0246
      TTY: (202) 727-3323

   b. **Training**

      1) The District Privacy Official, in conjunction with DOC, shall ensure that each DOC employee, contractor or future incumbent who may have access to or use of protected health information shall receive training on Privacy Policies and Procedures, as necessary and appropriate to carry out his or her job functions. Training shall be documented.

      2) The District Privacy Official, in conjunction with DOC, shall ensure that employees shall receive training no later than 45 days after there is material change in their job functions or in Privacy Policies and Procedures that affect their access to or use of protected health information.

      3) DOC shall ensure that employees receive annual refresher training regarding HIPAA requirements. Employees who are directly responsible for using and disclosing PHI shall receive annual specialized refresher training.

2. **DIRECTOR.** The Director for DOC has delegated the following authorities for implementation and oversight for this directive.

   a. **HIPPA Project Manager.** The Health Services Director is the HIPAA Project Manager, responsible for:

      1) Providing contract administration and assurance that health care business associates comply with HIPAA Privacy Rules.

2) Providing oversight for the implementation and management process.

3) Liaison with the District HIPAA Project Manager, DOC and its health care business associates.

b. **Internal Controls, Compliance and Accreditation Manager**

1) The OICCA Manager is designated, under the advice and concurrence of the District's Privacy Official, to amend DOC Privacy Policies and Procedures as necessary to comply with each material change in the Privacy Rules of other applicable federal or state law; or for internal business purposes, provided this type of amendment remains in compliance with the Privacy Rules and all other applicable federal and state privacy law.

2) OICCA shall conduct periodic monitoring of the ePartners Automated tracking and accounting database for compliance with this directive.

3) OICCA shall conduct an annual audit of compliance with this directive.

c. **The Privacy Officer.** The Privacy Officer is granted the authority to release or deny access to records and information within the agency in accordance with this directive. The Privacy Officer shall:

1) Provide oversight and technical assistance for adherence to HIPAA and this directive.

2) Monitor and ensure each DRS is identified and that contact information is published as to the location and accessibility of each record of the DRS (Attachment A).

3) Monitor and ensure DOC has identified the titles and locations of persons or offices responsible for receiving and processing PHI access requests, the access response, and any other documentation regarding compliance with obligations to provide access (Attachment A).

4) Monitor and ensure DOC and its business associates document each designated record set (DRS) that it maintains.

5) Maintain a record of activities pertaining to disclosure or non-disclosure of HIPAA-related activities. The record of activities includes written documentation of disclosure as well as documentation in the E-partners automated accounting and tracking database.

6) Submit annual report of activities to the Director no later than October of each year, with a copy provided to the HIPAA Project Manager and the Internal Controls Manager.

7) Coordinate all HIPAA training requirements with the DOC Training Administrator as outlined in Chapter 2, Section 1. "b."

3. **CONTRACTS.** Contracts shall contain requirements, promulgated by D.C. Office of Contracting and Procurement, to ensure compliance with the requirements imposed by Freedom Of Information Act (FOIA). The contracting component shall be responsible for ensuring that the contactor complies with requirements relating to the release of information and records in accordance with the FOIA and this Program Manual.

4. **DOC BUSINESS ASSOCIATES.** Each affected business associate shall:

a. Safeguard PHI and develop appropriate security procedures.

b. Use and disclose PHI in strict compliance with HIPAA Privacy Rules and this directive.

c. Ensure employees with access to PHI are adequately trained on the maintenance, use and disclosure requirements of HIPAA Privacy Rules and this directive.

5. **EMPLOYEES**

a. **Compliance.** Each employee authorized to use and disclose protected health information shall, at all times, comply with the policies and follow the procedures set out in this directive and shall consult with the agency head, or designee, if there is any doubt regarding whether such use or disclosure is permitted.

b. **Noncompliance.** Failure to comply with the policy may subject the employee to:

1) **Administrative Discipline**

a) DOC may impose discipline in accordance with sanctions set forth in Chapter 16 of the DPM and applicable collective bargaining agreements.

b) The health care business associates may impose discipline in accordance with their personnel rules and any contractual rules for discipline.

2) **Civil Penalties**. The Office of Civil Rights can impose penalties of $100 per infraction, up to $25,000 annually per standard.

3) **Criminal Penalties**. Fines up to $250,000 and/or imprisonment for up to ten years.

c. **Reporting Privacy Violations**

1) Each employee is obligated to promptly report any suspected violation of policies and procedures regarding the safeguard, use and disclosure of PHI, Privacy Rules and/or other applicable federal or state privacy law.

2) The report shall be appropriately made to the DOC Director or designee and the DOC Privacy Officer. If the reporting employee is a member of a business associate's workforce, they shall also notify the Chief Administrator.

3) Reports may be made anonymously.

4) Each employee shall cooperate fully with any investigation, corrective action or sanction instituted by the DOC Privacy Officer.

d. **Cooperation.** Each employee shall cooperate fully with efforts, to include contingency plans to mitigate, to the extent possible, any deleterious effect of improper use or disclosure of protected health information by a member of the DOC workforce or by a DOC business associates in violation of these privacy policies and procedures.

e. **Non-retaliation**

1) Employees are prohibited from attempting to intimidate, threaten, coerce, discriminate against or retaliate against an individual who:

a) Exercises any right, including filing complaints, under the Privacy Rules or other privacy laws.

b) Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by HHS or other appropriate authority.

c) Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rules (provided the opposition is reasonable and does not involve illegal disclosure of protected health information).

2) Each employee who suspects that another employee has violated the ban on retaliatory acts shall report the suspicion.

3) The report shall be appropriately made to the DOC Director or designee and the DOC Privacy Officer. If the reporting employee is a member of a business associate's workforce, they shall also notify the Chief Administrator.

4) Reports may be made anonymously.

5) Employees shall cooperate fully with any investigation, corrective action or sanction instituted.

CHAPTER 3

PROTECTED HEALTH INFORMATION
(Designated Record Sets)

1. **PROTECTED HEALTH INFORMATION (PHI).** Medical records; created, used, maintained and disclosed between DOC and its business associates; are primarily documentation of the care and treatment of inmates. This PHI is predominantly maintained in the medical record and is generally outlined in *DOC – HIPAA FORM 5 Medical Designated Record Set* (Attachment A-1). Limited PHI as outlined in *DOC – HIPAA FORM 5 Inmate Institutional Designated Record Set* (Attachment A-2) can be found in the inmate's official institution record.

2. **MEDICAL RECORDS.** PHI is usually contained in the inmate's medical record.

   a. The health care provider shall establish a medical record for each inmate committed to the CDF and the Correctional Corporation of America Correctional Treatment Facility (CTF).

   b. Medical data regarding the inmate shall be maintained in this confidential record.

   c. To enhance patient confidentiality, designated medical personnel shall be the only authorized personnel to handle medical records.

   d. The confidentiality of inmate PHI is set forth in compliance with laws, regulations and standards, and in accordance with policies and procedures that comply with DC Privacy and DOC confidential records management requirements.

   e. Although the medical record is the property of the DOC, the affected business associates shall control access to the record consistent with DC Privacy Rules, this directive and the affected business associate's policies.

   f. If the inmate is being transferred to the CCA/CTF, the health care provider shall forward the medical record in a sealed plastic envelope. Only an authorized health care employee shall open the sealed envelope.

3. **OFFICIAL INMATE INSTITUTIONAL FILES**

   a. Sometimes PHI is found in the inmate's institutional record or other DOC administrative files because it is summarized in another report or attached to the report. Some examples are; incident reports that include staff observations, injury reports, parole and work release reports when an

evaluation is being made to determine the inmate's readiness for community release and/or when on-going care will be required upon release.

b. Official inmate institutional files are classified as confidential and shall be preserved, protected, retained and disposed of in accordance with applicable laws, regulations, rights of privacy and DOC policy and procedures at PS 4060.2A "Inmate Record", (2/15/00). Further, PS 4060.2A "Inmate Record Security", § d. limits employee access and handling of this file. This policy complies with DC Privacy requirements.

4. COMMON TYPES OF PROTECTED HEALTH INFORMATION IN THE DESIGNATED RECORD SETS

a. Designated Record Set (Medical)

1) Medical Problem List

2) Physician Notes detailing patient progress

3) Nursing Notes

4) Mental Health Unit Forms (Does not include psychotherapy notes)

5) Dental Progress Notes and X-Rays

6) Consultation Notes from external providers

7) Referral Notes

8) Tuberculosis Documentation

9) Radiology Reports

10) Laboratory Results

11) Medication Administration Records

12) Inmate Injury Reports

13) Correctional Transport Forms to health care facilities

14) Emergency/Urgent Care Encounters Forms

15) Doctors Orders

16) X-Rays

17) Psychiatric Progress Notes

18) Wound Care Forms

b. **Designated Record Set (Non-Medical)**

1) Judgment and Commitment Orders (Medical/Mental Health Alerts from Judge)

2) Incident Report of Bizarre/Unusual Behavior

3) Automated Notification of Significant or Extraordinary Events

4) Injury Reports

5) Classification for Medical Reasons

6) Drug Test Results

7) Psychological Evaluation for Release Readiness

8) Psychological Tests – raw data

CHAPTER 4

SECURITY FOR PROTECTED HEALTH INFORMATION (PHI)

1. **INFORMATION SECURITY.** HIPPA requires that covered entities provide reasonable safeguards for the protection of PHI when it is being electronically stored or transmitted or otherwise maintained. In accordance with PS 2420.2 "Information Security", DOC shall maintain standard procedures for the security, management and control of the DC Department of Corrections (DOC) information and information systems by:

   a. **Access Paths and Systems.** Employing flow control systems, including firewalls, to protect information system resources. The establishment, modification, and termination of network connections shall be centrally managed and controlled by Office of Management Information and Technology Services (OMITS) on an ongoing basis.

   b. **Dial-Up Communications.** OMITS shall control access to and from information systems via dial-up connections. OMITS shall enforce standard policies and procedures governing both the location and employment of telephone modems.

2. **DISASTER RECOVERY PLAN**

   a. In accordance with PS 2420.8 "Disaster Recovery Plan, disruption of information service to users shall be avoided. This plan is "Agency Confidential", and contains procedures that will protect against the loss of automated data processing files, data in DOC's databases and servers, applications and systems software, systems documentation, and processing instructions.

   b. Each covered entity that electronically stores PHI shall develop disaster recovery/contingency plans for their IT systems.

   c. The Office of Management Information and Technology Services (OMITS) shall ensure that IT can continue to operate and communicate in an event of disruption of services or a major disaster.

   d. OMITS shall establish an IT operational capability to process data, implementation of work around solutions for those portions of the system which cannot be immediately restored, and ultimately, restoring IT processes to normal operational status.

3. **GENERAL REQUIREMENTS.** Storage, copying, handling, transmission and disposal of protected health information, including the media used to store PHI, shall be controlled in accordance with this directive.

   a. **Information Privacy – General Rules.** All members of the workforce shall vigilantly watch for and create an attitude and atmosphere of confidentiality.

   b. **Incidental Use and Disclosure**

      1) All members of the workforce may at some point be exposed or legitimately involved in the incidental use or disclosure of PHI about an inmate. For example, information may be contained in an incident report, the inmate may self-disclose information or the employee may overhear a conversation. *Employees shall not repeat this information to anyone.*

      2) Employees who are authorized to use and disclose PHI shall also use good judgment when using or disclosing protected health information in conversation, by mail, electronic transmission or any other means, and when recording and storing protected health information in any medium, to ensure that incidental use or disclosure of the protected health information in connection with an otherwise permitted or required use or disclosure is reasonably kept to a reasonable minimum.

   c. **Verbal communications**. If an employee is authorized to use and disclose PHI, it is to be done so as follows:

      1) Health care providers and other authorized employees shall only communicate the minimum necessary protected health information to another authorized employee or business associate on a need-to-know basis and only during the official conduct of their duties.

      2) Health care providers and other authorized employees shall ensure that any verbal exchange of protected health information is communicated in a confidential manner so that other employees and inmates do not become privy to the information.

   d. **Custody and Storage.** All employees shall adhere to the following safety precautions:

      1) Maintain custody and surveillance of files containing PHI.

      2) Never leave PHI unattended on desks, at photocopiers or printers.

      3) Lock file cabinets containing PHI whenever away from that storage area.

4) Never leave portable media containing PHI (e.g., diskettes, CDs and paper-copy) unsecured when it is not being used.

5) Log off or ensure security screen features are engaged whenever leaving their personal computer/workstation unattended.

e. **Telephone**

Restrict verbal transmission of PHI unless the authorized employee can establish that they personally know the receiver is authorized to use and disclose the requested information or that the requester has submitted required identification and verification of authority.

f. **Faxing**

1) Ensure that the person who is receiving the facsimile containing protected health information is authorized to use and disclose it.

2) Always use a PHI cover fax page. The following confidentiality statement shall be incorporated into all fax transmissions that contain PHI:

> **"PRIVACY/CONFIDENTIALITY NOTICE (PHI)**: The information in this transmission contains protected health information in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This message is intended only for the use of the individual to which it is addressed and contains information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. Violation of Privacy Rules may result in civil and criminal penalties consistent with CFR 164.512(k)(5)(iii). If you are not the intended recipient, please contact the sender by email, fax or phone and destroy all copies of the original message."

3) Take precautions to avoid misrouting.

4) Make every effort to notify the intended receiver in advance that transmission is imminent.

5) If the fax machine is not in a secured area, stay with document until it is scanned and immediately remove and return it to its secure file.

g. **Copying**

1) Ensure that the person making the copy is authorized to use and disclose protected health information.

2) If the copier is not in a secured area, stay with the document until it is copied and immediately remove and return the PHI to its secure file.

h. **Email.** Protected health information may be transmitted via e-mail in accordance with protective measures required in this directive.

1) The following confidentiality statement shall be incorporated into all e-mail transmissions that contain PHI:

> **"PRIVACY/CONFIDENTIALITY NOTICE (PHI)**: The information in this transmission contains protected health information in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This message is intended only for the use of the individual to which it is addressed and contains information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. Violation of Privacy Rules may result in civil and criminal penalties consistent with CFR 164.512(k)(5)(iii). If you are not the intended recipient, please contact the sender by email, fax or phone and destroy all copies of the original message."

2) Employees shall log out from their personal computer upon completion of the task when it contains PHI.

i. **Personnel Changes**

1) Business associates shall immediately notify in-house managers, affected business associates, the DOC Privacy Officer, and other appropriate DOC managers when personnel changes (e.g., reassignments, changes in job responsibilities/titles, terminations, authorization or restrictions of use and disclosure of PHI and any other changes) affect use and disclosure of protected health information.

2) DOC supervisors shall immediately notify the DOC Privacy Officer, OMITS, and the affected business associates of DOC personnel

changes (e.g., reassignments, changes in job responsibilities/titles, terminations, authorization or restrictions of use and disclosure of PHI and any other changes) that affect use and disclosure of protected health information.

CHAPTER 5

PERMITTED USES AND DISCLOSURES

1. TERMS

a. **Use** means the **in-house** sharing, application, utilization, examination, or analysis of PHI within the normal treatment and operational activities of the DOC between covered entities. Covered entities include authorized DOC workforce and contract hospital and health care providers and correctional custodial providers). Particular job functions are authorized to:

1) **Use** PHI in medical databases or on various forms.

2) **Use** PHI when answering questions from treatment providers within the covered entities, or on the phone or in Email about services performed to/for inmates.

3) **Use** PHI when communicating with, responding to medical requests from/to other covered entities under HIPAA Privacy Rules (example: Greater SE Community Hospital, DC Chartered Health Care, Addiction Prevention and Recovery Administration, DOC or CCA/CTF managers).

4) **Use** when communicating during a Housing Board Hearing (for example: about an inmate's injuries related to a suspected assault).

b. **Disclosure** means the release, transfer, provision of access to, or divulging in any other manner of PHI **outside** of the covered entity roof. For example:

1) **Disclosure** by sending PHI to a government agency that could be part of normal reporting on routine and recurring tasks as part of scheduled reporting activities (for example: DOH, DHHS, FBOP).

2) **Disclosure** when required by a court order or subpoena to produce copies of an inmate's institutional or medical record/information from DOC or the health provider's records.

3) **Disclosure** to the inmate's personal representative.

4) **Disclosure** to a former inmate, that inmate's personal representative or to that individual's private physician.

2. **PERMITTED USE AND DISCLOSURE.** Under HIPAA, DOC and the covered entities may use and disclose Protected Health Information (PHI) without the inmate's permission as follows. Disclosure that is outside of these conditions requires authorization and is further covered in Chapter 6, *Exceptions to Permitted Disclosure* of this directive. The inmate's *authorization is not required for use and disclosure of PHI in the following instances*:

   a. **Business Associates.** No authorization from the inmate is necessary for business associates to use PHI on behalf of DOC, nor for DOC to disclose PHI to the business associates.

   b. **Internal treatment and health care operations.** Generally the use and disclosure of minimum necessary protected health information shall be the responsibility of the health care provider or CTF business associate in conjunction with the DOC Privacy Officer. However authorized DOC staff or other business associates may disclose PHI contained in the inmate's institutional file or similar record. In all cases, use and disclosure shall be in accordance with Health Information Privacy, other applicable laws, regulations and standards, this directive, applicable DOC requirements and the health care provider's policies that are consistent with HIPAA.

   c. **Disclosures of PHI to other health care providers.** The Department of Corrections, or its business associates who provide health care and who use and disclose protected health information to other health care providers for treatment purposes are not limited to the "minimum necessary" guidelines.

   d. **For uses and disclosures about public health and safety threats.** Use and disclosure of information to law enforcement to prevent or lessen a serious and imminent health or safety threat to a person or the public provided there is reasonable belief that the use or disclosure involves a person (including the target) who is able to prevent or lessen the threat or to identify or to apprehend an individual who appears from the circumstances to have escaped from a correctional institution or lawful custody, or we reasonably believe may have caused serious physical harm to a victim, based on the individual's statement admitting participation in a violent crime.

   e. **For uses and disclosures for public health, public interest and public benefit.** Only the minimum necessary protected health information shall be used or disclosed for the particular public health or benefit activity involved to include public health authority legally authorized to collect or receive protected health information to prevent or control disease, injury or disability (including disease, injury, birth, death, other vital event reporting, and public health surveillance, investigation or intervention).

   f. **To report adverse events (usually to the Food and Drug Administration (FDA).** The minimum necessary protected health information shall be used or

disclosed for activities related to the quality, safety or effectiveness of a FDA–regulated product or activity to persons subject to FDA jurisdiction with responsibility for that FDA–regulated product or service, including to collect or report adverse events (or similar activities regarding food or dietary supplements); product, product use or labeling defects or problems; or biological product deviations; to enable product recalls, repairs, replacements or look-backs (including locating and notifying individuals who received the products); track FDA–regulated products; conduct post–marketing surveillance.

g. **For disclosures about persons exposed to communicable diseases.** The minimum necessary protected health information shall be disclosed to persons who may have been exposed to communicable disease, or who are otherwise at risk of contracting or spreading disease, when DOC or a public health authority is legally authorized to give notification as needed in conducting public health intervention or investigation.

h. **For disclosures about victims of abuse.** For the purposes of this directive, the minimum necessary protected health information shall be used and disclosed when there is reason to believe an abuse has been committed within the confines of the DOC or when requested from law enforcement pursuant to Sections "i." through "k." below.

i. **For disclosures for health oversight activities.** The minimum necessary protected health information shall be disclosed to a health oversight agency as needed for legally authorized health oversight activities, such as audits, civil, criminal or administrative actions or proceedings, inspections, licensure, certification, disciplinary actions, and appropriate oversight of the health care system or government benefits programs (e.g., Medicare and Medicaid) for which health information is relevant to beneficiary eligibility or entities subject to government regulatory programs or civil rights laws.

j. **Judicial and administrative law proceedings.** Authorized employees may disclose the minimum necessary protected health information to the court of a judicial or administrative proceeding; in response to a court or administrative tribunal order, provided only the expressly ordered protected health information is disclosed. Additionally, authorized employees may disclose the minimum necessary protected health information in response to a subpoena, a court order, discovery request or other lawful process not accompanied by court or administrative tribunal order, when DOC has made a reasonable effort to provide notice to the individual sufficient to permit the individual to object to, or seek a qualified protective order from, a court or administrative tribunal or there is "satisfactory assurance" that the information seeker has made reasonable efforts either (a) to ensure the individual has notice, or (b) to secure a qualified protective order from the court or administrative tribunal or by party stipulation that limits the parties'

use or disclosure to the purpose of the proceeding, and requires return or destruction of the protected health information (including all copies) at end of the proceeding.

k. **Law enforcement purposes**

1) The minimum necessary protected health information may be disclosed to a law enforcement official in compliance with a judicial order, warrant, summons, regular or grand jury subpoena. The minimum necessary protected health information shall be disclosed to a law enforcement official in compliance with an administrative subpoena, summons, request, civil investigative demand or similar process. However the PHI shall be specific and limited in scope to that which is relevant and material to a legitimate law enforcement inquiry, and when other non-PHI can be used.

2) Disclosure, unless required by law, shall not be made about DNA, DNA analysis, dental records, or body or tissue typing, samples or analyses (other than blood type).

3) The minimum necessary protected health information shall be used and disclosed when furnishing health care in a medical emergency (other than an emergency on the premises) if the disclosure appears necessary to alert law enforcement officials of commission and nature of a crime, the location of the crime and its victims, and the identity, description, and location of suspected criminals.

4) The minimum necessary protected health information shall be disclosed to a law enforcement official seeking information about an actual or suspected crime victim.

l. **Required by law.** PHI shall be used and disclosed to a law enforcement official as required by law, including to report wounds or physical injuries. There is no minimum necessary limitation for use or disclosure of protected health information required by law, but the use or disclosure shall comply with and be limited to the relevant legal requirements, and all applicable legal procedural requirements shall be followed.

m. **Mental Health.** The following PHI may be used or disclosed for treatment, prerelease and post release care. Inmates are required to sign an authorization to release information to community health care providers and other release programs.

1) Medication prescription and monitoring.

2) Counseling session start and stop times.

3) Modalities and frequencies of treatment furnished.

4) Results of clinical tests.

5) Any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

n. **Correctional institution or law enforcement official**

1) On a need-to-know basis, disclosure of the minimum necessary protected health information regarding an inmate or individual in lawful custody may be made to a correctional institution or a law enforcement official, if the correctional institution or law enforcement official represents that the protected health information is needed to:

a) Ensure the health and safety of the inmate, other inmates, officers, employees or others at the correctional institution or responsible for transporting or transferring inmates to other correctional institutions or facilities.

b) For the administration and maintenance of correctional institution's safety, security and good order.

2) Notations shall be made in the inmate's electronic or paper medical record indicating whether the inmate is free of communicable and/or infectious disease for the purpose of screening for an institutional work assignment in accordance with policy and procedures in DOC PS 4740.1C "Culinary Workers – Examination and Daily Workers Inspection" (1/12/01). The inmate's name and DCDC# maybe included on the Medical Clearance for work memo to ARAMARK.

3) PHI and a referral for specialized housing within the Central Detention Facility based upon the health care providers diagnosis of the inmate's physical or mental condition, shall respectively be handled in accordance with DO 3800.2 "Section 504 Handicap/ Americans with Disabilities Act Accommodations" (8/10/92) and the Post Order for South Three – Mental Health Unit.

o. **Suspicious deaths or other crimes within the DOC.** The minimum necessary protected health information shall be disclosed to alert a law enforcement official about an individual's death that is suspected to be the result of criminal conduct or when there is good faith belief that the protected health information constitutes evidence of criminal conduct within DOC facilities.

p. **Decedents (to a coroner or medical examiner).** The minimum necessary protected health information shall be disclosed to a coroner or medical examiner for identifying deceased persons, determining cause of death or their other legally authorized duties. Protected health information shall be

disclosed to funeral directors, consistent with applicable law, as necessary for them to carry out their duties.

q. **Foreign Government.** Protected health information shall be disclosed at the direction of a public health authority, to a foreign government official acting in collaboration with a public health authority.

r. **Research purposes.** Disclosure of the minimum necessary protected health information for research shall be made in accordance with instructions in chapter 7, section 9 of this directive.

s. **Informed Consent for general research purposes** is covered in DOC PS 1311.1C "Management Controls – Research Activity" (5/20/02).

t. **Specialized government operations (to include Corrections and Jails).** Disclosure of the minimum necessary protected health information shall be made to authorized federal officials for lawful intelligence, counterintelligence, and national security activities.

u. **Public Health and Safety Threats.** Consistent with applicable law and ethical standards, use or disclosure of the minimum necessary protected health information believed, in good faith is to be used to prevent or lessen a serious imminent health or safety threat to a person or to the public.

v. **Disaster Relief.** DOC and its business associates may use and disclose to a public or private entity, authorized by law or charter to assist in disaster relief, the minimum necessary protected health information to coordinate notifying (including identifying or locating) an individual's family members, personal representatives or other persons responsible for the individual's health care, of the individual's location, general condition or death. DOC and its business associates shall follow all applicable procedures unless the Director or other authority determines, that following the applicable procedures will interfere with the public or private entity's ability to respond to the emergency circumstances.

w. **Individual Not Present or Emergency.** When (a) the individual is absent, unavailable, incapacitated or dead, or (b) there is an emergency making advance notice and the opportunity for the individual to restrict or object impractical, DOC may use the individual's PHI with and disclose it to persons involved with the individual's health care (but not persons involved only with payment related to that health care) or disaster relief if DOC determines, in its professional judgment, that the use and disclosure will be in the individual's best interest. DOC may use or disclose only the minimum necessary protected health information directly relevant to the person's involvement with the individual's health care or disaster relief.

x. **Official Inmate Institutional Files**

DOC may use and disclose limited protected health information (PHI) that is maintained in DOC files outside of the inmate medical record. This may include but not be limited to incident or other reports of the inmate's physical and mental health, medical release plans, medication requirements, psychological evaluations that may be incorporated into parole and other release reports or in reports to the courts as required by law to aid in sentencing.

y. **Workers' Compensation**

HIPAA provides that DOC and its covered business associates shall disclose protected health information about employees that is authorized by and needed to comply with workers' compensation or similar programs established by law that provide benefits for work–related injury or illness without regard to fault. Procedures for disclosure of injury reports is provided in DO 2921.2 "Reporting On-the-Job Injuries" (6/25/82).

CHAPTER 6

EXCEPTIONS TO PERMITTED DISCLOSURE – DENIAL OF ACCESS

1. Inmates, their personal representative or a former inmate may be denied access to the information, without being provided the opportunity for review of the reason for the denial.

2. PHI that may be denied access without opportunity for review of the decision are as follows:

   a. The individual does not have the right to inspect the information, or it is otherwise prohibited or protected by law.

   b. Information requested is in reasonable anticipation of or for use in civil, criminal or administrative action or proceeding.

   c. The PHI was obtained in confidence from a source, other than a health care provider, and it can be reasonably demonstrated that access would reasonably likely reveal the source.

   d. The PHI was withheld from the individual under the Clinical Laboratory Improvements Amendments of 1988 (42 U.S.C. § 263a).

   e. The requested PHI is Psychotherapy notes.

      1) The health care provider compiled the PHI in the course of continuing research, including treatment, and the individual agreed to waive access when consenting to participate in the research. Access will be reinstated when the research is completed.

      2) The PHI is restricted from disclosure under the Federal Privacy Act (5 U.S.C. § 552a).

      3) A licensed health care professional, in exercise of professional judgment, has determined that the PHI is reasonably likely to:

         a) Endanger the life or physical safety of the individual or another person.

         b) Cause substantial harm to a person, not a health care provider, who is referenced in the protected health information.

         c) Cause substantial harm to an individual or another person, if a personal representative's access request were granted.

CHAPTER 7

INMATE REQUEST FOR ACCESS TO PHI

1. **ASSISTANCE TO ACCESS PHI.** When a literacy or language problem prevents an inmate from understanding consent to release of PHI or how to access his/her PHI, a staff member shall assist the inmate. Appropriate assistance may include, but is not limited to providing assess to:

   a. **Translator Services**

      1) A staff member, who has been determined to be proficient in the affected inmate's language, may be designated the authority to assist the inmate in accessing PHI in accordance with this directive.

      a. Language Line Service (LLS). This service may be used to assist the inmate and authorized staff to communicate during access and disclosure of PHI.

      2) Translating services for deaf and hearing impaired inmates shall be handled in accordance with PS 3800.3 "ADA: Communications for Deaf and Hearing Impaired" (9//30/03).

   b. **Privacy Officer.** When an employee who is authorized to use and disclose PHI is unable to further assist the inmate in understanding the provisions of this directive or the questions are beyond the expertise of the employee, the employee may request the assistance of the DOC Privacy Officer.

2. **INMATE ACCESS TO PHI IN THEIR MEDICAL RECORD.** The health care provider shall allow inmates access to PHI in their medical record in accordance with HIPAA law, this directive, PS 1300.1B "FOIA" (12/15/03) and CCHPS 800.0 "Medical Records Confidentiality" (4/12/03).

   a. Inmates shall request review of particular documents or their entire medical record by submitting a *DOC-HIPAA FORM 38A Request to Access PHI* (Attachment B) to the CCHPS Records Officer.

   b. The Medical Records Officer shall schedule the records review within five days (excluding weekends and holidays) of receipt of the request.

   c. Prior to the inmate's review, authorized medical staff shall review the requested PHI to determine if the requested PHI is eligible for disclosure pursuant to this directive.

d. **Risk or Harm if PHI is disclosed.** If a document contains PHI; that is determined to jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of any officer, employee or other person at the correctional institution or responsible for transporting the inmate, the employee shall:

1) Make a photocopy of the affected document and store the original in separate folder used to temporarily store PHI that will not be disclosed.

2) Black/blot out the PHI on the photocopy that will not be disclosed.

3) Place the photocopy in the medical record.

4) The inmate shall be allowed to review the remainder of the medical record.

e. **Evaluative Information.** If subjective evaluations and opinions of medical staff relating to the inmate's care and treatment are contained in outpatient notes, consultation reports, narrative summaries or reports by a specialist, operative reports by the physician, and summaries by specialists as the result of laboratory analysis, or in-patient progress reports; a medical officer, in consultation with the DOC Privacy Officer shall determine disclosure.

1) The same procedures outlined in Section c. above shall be implemented.

2) The inmate shall be allowed to review the remainder of the medical record.

f. **Inmate Supervision.**

1) The Medical Records Officer shall provide adequate space to allow the inmate to review his or her medical file.

2) During review of PHI contained in the medical record, the inmate shall remain in sight and sound supervision.

3) The inmate shall not be allowed to take notes or to receive copies of PHI.

g. **Documentation.** Review and documentation of disclosures shall be recorded and maintained in the medical records and DOC Privacy Officer's file. Procedures for documentation are provided in Chapter 9.

3. **INMATE ACCESS TO PHI IN THEIR OFFICIAL INSTITUTIONAL RECORD**
Generally, PHI contained in the inmate's official institutional record is "incidental" because it is obtained from medical files and is generally limited to such

documents as injury reports, a statement in a housing board or disciplinary reports that relates to an injury that occurred, a medical alert contained in a commitment document, a statement pertaining to the inmate's release readiness that is contained in a progress report or a consent to release of information form.

a. The Case Manager is usually the designated employee who supervises an inmate when the inmate is reviewing their official institutional record.

b. The inmate shall submit *DOC-HIPAA FORM 38A* to the Case Manager.

c. The Case Manager shall schedule the records review within five days (excluding weekends and holidays).

d. Prior to the inmate's review of the record, the Case Manager shall review the file to determine if PHI is contained in the institutional record.

e. If PHI is contained in the institutional record, the Case Managers shall consult with the medical records officer and the DOC Privacy Officer to determine if review of this information would present a risk of harm or potential risk to either the inmate or other individuals.

f. If a document contains PHI; that is determined to jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of any officer, employee or other person at the correctional institution or responsible for transporting the inmate, and the inmate has requested a copy of the document; the PHI shall be blacked/blotted out prior to the copy being made.

g. If the DOC Privacy Officer determines that any portion of PHI shall not be disclosed on this basis, the inmate shall be so advised in writing and provided the address to which the inmate may address a formal request for the withheld records.

h. The inmate shall be allowed to review the remainder of the institutional record to include any disclosed PHI in accordance with FOIA and any other applicable security restraints regarding disclosure.

i. However, the inmate shall not be allowed to take notes or receive copies of the PHI that is contained in the file.

CHAPTER 8

PROCEDURES FOR DISCLOSURE OF PHI

1. **REQUEST REVIEW.** The health care provider, other business associate or DOC employee authorized to disclose the requested PHI shall review each request for access to PHI and disclose the minimum necessary PHI in accordance with this directive.

2. **DOC PRIVACY OFFICER.** When needed or if stipulated in this directive, the employee shall consult with the DOC Privacy Officer and/or Health Services Administrator. The provider shall, upon approval for disclosure, review the record and obtain the PHI necessary to respond to the request.

3. **PERMITTED USE AND DISCLOSURE.** The inmate's consent is not required for use and disclosure pursuant to provisions detailed in Chapter 5, "Permitted Uses and Disclosures", Section 2.

4. **CONSENT TO RELEASE PHI TO A THIRD PARTY** Minimum Necessary PHI may be disclosed when the inmate has issued written consent as follows:

   a. Inmates may request or consent to release of PHI to their attorney-of-record in accordance with Privacy Rules, this directive and as outlined in CCHPS Policy 800.0 "Medical Record Confidentiality" (4/12/03) and PS 1300.2A "Consent to Release Information" (12/15/03).

   b. Inmates may request and/or consent to release of PHI to community based programs for future treatment or release assistance in accordance with this directive. Procedures are outlined in CCHPS Policy 800.0 "Medical Record Confidentiality" and supported in PS 1300.1B "Freedom of Information" (12/15/03) and PS 1300.2A "Consent to Release Information" (12/15/03).

   c. The inmate shall submit the consent to disclose PHI, using *DOC -- HIPAA FORM 3 Consent to Disclose PHI Section A* to the staff member who is authorized to disclose the PHI as set forth in Chapter 7 "Procedures for Disclosure".

   d. The inmate shall list all requested PHI to disclosed in the consent.

   e. The form shall contain an expiration date, or expiration event (e.g., "end of research protocol").

   f. The form shall contain the inmate's signature and date, (and if signed by the personal representative—authority to act for the inmate).

g. PHI that has been determined to jeopardize safety and security as described in Section 3 of this Chapter shall not be released without the written permission of the DOC Privacy Officer.

h. The employee who is authorized to disclose the PHI shall place a copy of *DOC-HIPAA FORM 3* in the record that contained the PHI and submit a copy to the DOC Privacy Officer.

i. In some cases when research is being conducted, the inmate may be required to first consent to use of his/her PHI.

5. **PERSONAL REPRESENTATIVE'S ACCESS TO PHI**

a. The inmate's personal representative as defined in this directive shall complete *DOC – HIPAA FORM 38A* to access PHI on behalf of the inmate. Attorneys of record are not personal representatives unless so appointed as the inmate's power of attorney or as appointed by the courts.

b. The inmate's personal representative shall not be given PHI that has been determined to jeopardize safety and security as described in Section 3 of this Chapter.

6. **REVOCATION OF CONSENT.** An inmate may revoke a consent at any time. Revocation of consent does not affect DOC's use/disclosure prior to learning of the revocation.

7. **FORMER INMATE'S REQUEST TO ACCESS INDIVIDUAL PHI.** Inmates who have been released from custody have the right to receive a copy of their PHI.

a. The requester shall obtain *DOC -- HIPAA FORM 38A Section A* from the DOC Privacy Officer.

b. The requester shall submit DOC-HIPAA FORM 38A to the DOC Privacy Officer.

8. **VERIFICATION OF IDENTITY.** Employees who are authorized to disclose PHI must ensure that it is *only* given to persons who are authorized to receive it.

a. Authorized employees and business associates (i.e., covered entities) shall document verification of identity in *Section B of DOC-HIPAA FORM 10 Disclosure Log/Authorization/ Verification/Minimum Necessary Requirement* (Attachment C).

b. If there are still questions regarding either verification of the requestor's identity or their authority to receive the requested PHI, the employee or

health care provider shall consult the DOC Privacy Officer before any disclosure is made.

c. Examples of appropriate identification include:

1) **Personal Recognition.** The employee who is authorized to disclose the PHI shall document on *DOC-HIPAA FORM 10*, Section B that the requestor's or receiver's identity is known and provide a brief statement of how this knowledge was determined.

2) **Documented Identification** such as:

a) Photographic identification card.

b) Government identification card or badge.

c) Appropriate document on government letterhead.

d) If a person purports to be acting on behalf of a public official, appropriate identification includes, if reasonable for the situation:

(1) A written statement of appointment on appropriate government letterhead.

(2) A contract, memorandum of understanding, purchase order or other evidence establishing the appointment to act on behalf of the public official.

9. **EVIDENCE OF AUTHORITY.** Evidence of authority shall be determined as follows:

a. Receipt of a DOC-HIPAA FORM 3 *Consent to Release PHI* that was completed and signed by:

1) The inmate.

2) The inmate's personal representative.

b. If not the inmate or the inmate's personal representative, establish and document on *DOC – HIPAA FORM 10 Section C*, if authority to received PHI is applicable. Examples of appropriate authority include, if reasonable for the situation:

1) A warrant, subpoena, order or other legal process issued by a grand jury, a court, or an administrative tribunal.

2) A written statement of legal authority or, with respect to a properly identified government official, an oral statement of authority, if reliance on such oral statement is reasonable for the situation. The authorized employee shall document the oral statement on *DOC – HIPAA FORM 10*, Section C.

3) Identification as legal guardian, executor or administrator with respect to a deceased individual or an estate, power of attorney or other evidence of legal authority to act on behalf of an individual with respect to health care, or other evidence of appropriate relationship with the individual with respect to health care.

10. **MINIMUM NECESSARY RULES.** In most cases, when using or disclosing PHI or when requesting PHI from another covered entity, limit PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure, or request.

a. **Exceptions to the Minimum Necessary Rules.** Minimum Necessary does not apply to:

1) PHI disclosure to, or requests from, a health care provider for treatment and internal operations.

2) Uses or disclosure granted and made when the inmate authorizes release.

3) PHI disclosures made to the DHHS Secretary for HIPAA compliance investigations.

4) Uses or disclosure of PHI that is required by law.

b. **Use and Disclosure of Minimum Necessary PHI.** Staff shall make reasonable effort to use, disclose and request only the minimum necessary PHI to accomplish the intended purpose of the request. The employee shall document on *DOC-HIPAA FORM 10* Section D when the minimum necessary rule does not apply.

c. **Routine and Reoccurring Requests.** Some requests for and disclosure of PHI are routine and reoccurring. Examples of routine and reoccurring requests are:

1) Requests from a covered entity that is subject to the Privacy Rules.

2) Request from a professional who is a member of the agency workforce or business associate, and that person represents that the minimum necessary PHI is being sought.

3) Request from a government agent or law enforcement official who represents that the minimum necessary PHI is being sought.

4) Request based upon an authorized DOC research or statistical activity that documents that the minimum necessary PHI is being sought.

d. **Evaluations and Progress Reports.** Psychological reports, medication requirements and other data or referrals made as part of an inmate's release plan.

e. **PHI Restrictions for Law Enforcement Purposes.** For the purpose of law enforcement regarding identification or location, the minimum necessary protected health information that may be disclosed is limited to not more than the following: Authorized employees shall release only the following PHI as specified below:

1) The individual's statement.

2) Name.

3) Address.

4) Social Security Number.

5) Date and place of birth.

6) Blood type.

7) Type of injury, date and time of treatment.

8) Distinguishing characteristics (e.g., height, weight, gender, race, hair and eye color, facial hair, scars, tattoos).

9) If applicable, death.

f. **Entire Medical Record.** When an entire medical record is requested by a party that is not a covered entity or the subject of the PHI, the health care provider shall:

1) Determine on an individual basis whether the situation justifies using, disclosing or requesting an entire medical record as the minimum necessary protected health information for the purpose. This in regards to when an inmate's personal representative or 3rd party requests to review the entire record.

2) Consult with the DOC Privacy Officer if the disclosure request is made by an individual other than the individual inmate to review his/her medical record.

3) The health care provider shall provide a summary or explanation of the requested protected health information if the individual requests and agrees to pay designated fees for preparing the summary or explanation.

4) The DOC Privacy Officer and the business associate shall maintain all disclosure logs and documentation that are required by HIPAA and set forth in Chapter 8 of this directive.

4. **NON-ROUTINE REQUESTS TO DOC PRIVACY OFFICER.** Requests for PHI that are not routine or reoccurring in the usual conduct of business operations shall be forwarded to the DOC Privacy Officer.

a. The DOC Privacy Officer shall process each access request in accordance with law, regulations, and policies and procedures.

b. The DOC Privacy Officer shall direct the business associate to furnish PHI needed to comply with the access request *using DOC – HIPAA FORM 38B Direction to Retrieve Records* (Attachment E).

c. The DOC Privacy Officer, in conjunction with the business associate, shall verify the identity and authority of the person from seeking disclosure.

d. The DOC Privacy Officer shall respond in writing to the individual's request for access to PHI within 30 days.

1) The initial response may be a written notice that a 30-day extension will be taken for reasons stated in the notice.

2) The DOC Privacy Officer shall track and record the request to access PHI, using *DOC – HIPAA FORM 38C Access Request Processing* (Attachment F).

e. The DOC Privacy Officer shall make, a final determination within 30 days or 60 days when a notice of extension was issued.

5. **GRANT OF ACCESS TO RECORDS**

a. If access is granted, the DOC Privacy Officer shall use *DOC – HIPAA FORM 38D Grant of Access to Records* (Attachment G), Section to provide notice and inform the individual of any applicable fees.

b. The Privacy Officer shall ensure that all disclosure forms are filed in the inmate's medical record, and/or institutional record when appropriate, and retain a copy in the privacy official file.

6. **DENIAL OF ACCESS**

a. Only the DOC Privacy Officer shall determine whether to grant or deny an individual access to protected health information.

b. The DOC Privacy Officer shall deny access to PHI.

c. The DOC Privacy Officer may deny access to PHI if a licensed health care professional has determined, in the exercise of professional judgment that:

1) The access requested is *reasonably* likely to endanger the life or physical safety of a current/former inmate or another person.

2) The PHI makes reference to another person (unless such other person is a health care provider) and the access requested is *reasonably* likely to cause substantial harm to such other person.

3) The request for access is made by an inmate's personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the inmate or another person.

d. When the DOC Privacy Officer denies access to protected health information, the DOC Privacy Officer shall:

1) Inform the individual in writing, using *DOC – HIPAA FORM 38E Denial of Access to Records* (Attachment H), about the reason that the information is being withheld from them. The denial shall include:

a) The basis for the denial.

b) The individual's review rights.

c) Instructions for exercising his/her review rights.

d) The instructions for filing a complaint with DOC or the Department of Health and Human Services (DHHS).

2) After denying a specific PHI request, DOC shall, to the extent possible, give the individual access to any other requested PHI that can be disclosed.

7. **RIGHT OF REVIEW.** If DOC denies access to PHI, in whole or in part, and the requester has the right to review the reason for the denial, the Privacy Officer or designee shall:

a. Forward the request to the DOC Health Services Administrator to review and designate a licensed health care professional who did not participate in the denial decision to review the decision and, within a reasonable time, report to the DOC Privacy Officer whether the denial is justified.

b. Promptly report the reviewer's determination in writing to the individual, and act in accordance with the reviewer's determination.

c. Inform the requester in writing of further appeal options.

8. **ACCESS FEES.** DOC does not charge for search and retrieval of PHI but may charge a reasonable cost-based fee for providing requested summaries pertaining to PHI, copying and mailing the requested PHI.

a. **Notification of Fees.** The DOC Privacy Officer shall inform the individual of accessed fees in advance so that the individual may elect to withdraw or modify the request to reduce or avoid the fee.

b. **Medical Record.** The District Government, upon the Privacy Officer's review and approval, may receive reasonable compensation for preparing a summary or explanation of the requested protected health information.

c. **Fee Assessment.** Fees for copies of PHI contained in either the medical file that is in the custody of the health care provider or PHI that is contained in the inmate's official institutional record are calculated as follows:

1) Inmates may be charged 0.10 per page. The DOC Privacy Officer shall have the discretion to waive a fee when the inmate is indigent.

2) Personal representative shall be charged a fee of 0.25 per page.

3) First class mailing fees shall be accessed based upon the weight of the documents.

4) Generally other government agencies and business associates shall not be assessed copying and mailing fees.

9. **RESEARCH STUDIES**

a. A request to conduct research about inmates (current/former) that includes use of PHI shall be submitted to the DOC Director in accordance with PS 1311.1C "Management Controls – Research Activity" (5/20/02).

b. In addition to documentation required in section a. above, the researcher shall submit *DOC -- HIPAA FORM 12, Research Access Request* (Attachment I).

c. The Office of Internal Controls, Compliance and Accreditation (OICCA) shall, in conjunction with the DOC Privacy Officer, recommend approval or denial

of the request in accordance with PS 1311.1C. When necessary, OICCA shall consult with the DOC Data Access Review Committee (DARC) for guidance.

d. When there is proper representation from a researcher that the protected health information is needed for the research, PHI shall be used and disclosed only as specifically needed to prepare the research protocol or for a similar preparatory purpose, and no protected health information shall be removed from the premises during the review.

e. Both the DOC Privacy Officer and OICCA shall maintain a copy of the research request and all other documentation in the file.

f. Required documentation is set forth in PS 1311.1C noting that at a minimum the following documentation is required.

1) The name of the research protocol or activity.

2) A plain language description of the research protocol or activity, including its purpose and criteria for selecting particular records.

3) A brief description of the type of protected health information disclosed.

4) The dates or period during which the disclosures occurred, or may have occurred, including the date of the last disclosure during the period covered by the individual's request.

5) The name, address, and telephone number of the research sponsor and the researcher to whom the disclosures were made.

6) A statement that the individual's protected health information may or may not have been disclosed for a particular research protocol or other research activity.

7) Assistance in contacting the research sponsor and the researcher, if it is reasonably likely that the individual's protected health information was disclosed for the research protocol or activity.

8) Estimated date that the research study will end.

CHAPTER 9
DISCLOSURE ACCOUNTING

1. **ePARTNERS AUTOMATED DOCUMENTATION AND TRACKING.** In addition to completion of *DOC-HIPPA FORM 10*, the authorized employee shall enter all relevant data for tracking PHI accounting, disclosures and complaints into the ePartners software program. This software generates complete disclosure logs, as well as information on each disclosure, as necessary.

   a. The website for DOC is: http://hipaaepartner.dev.in.dc.gov/hipaa.

   b. The authorized employee shall use their designated computer identification name and password for entry and review. At a minimum the following information shall to be entered:

      1) The disclosure date.

      2) Inmate's Name.

      3) Inmate's DCDC #.

      4) The name and address of each person or entity that received the response.

      5) Social Security Number or other identifier if recipient is not the inmate.

      6) Type of authorization or disclosure.

      7) Verification of Recipient's Identity and Authorization to receive PHI.

      8) A description of the PHI disclosed.

      9) A statement of purpose for the disclosure and/or a copy of any written request for the disclosure.

   c. **Disclosure to be Documented.** Although documentation of disclosure of most of the following PHI is not required by Privacy Rules, DOC has determined that disclosure shall be documented for logging and tracking purposes. However, disclosure accounting to the individual subject shall only be made in accordance with Privacy Rules and this directive.

      1) Disclosures made to the inmate or personal.

      2) Disclosures made pursuant to the inmate's authorization.

      3) Disclosures required by law.

      4) Disclosures made to persons involved in the inmate's health care.

5) Disclosures for public health and health oversight activities.

6) Disclosures for FDA adverse event reporting.

7) Disclosures to a person who may have been exposed to a communicable disease as defined in Chapter 5, Section g.

8) Disclosures to a government authority about victims of abuse.

9) Disclosures for judicial and administrative proceedings.

10) Disclosures pursuant to a court order or subpoena.

11) Disclosures for law enforcement purposes (physical injuries, pursuant to court order or subpoena or summons, pursuant to a grand jury subpoena).

12) Disclosure in response to a law enforcement official's request regarding victims of a crime.

13) Disclosures to law enforcement about deaths of inmates suspected as the result of criminal conduct.

14) Disclosure to law enforcement about criminal conduct on DOC premises or in emergency situations.

15) Disclosures made to correctional institutions or law enforcement officers regarding inmates or individuals in lawful custody.

16) Disclosures about decedents to a coroner or funeral director to carry out their duties.

17) Disclosures to avert a serious threat to health or safety.

18) Disclosures for research purposes when there is a valid waiver.

19) Disclosures for specialized government functions.

20) Disclosures made for national security or intelligence purposes.

2. **DISCLOSURE ACCOUNTING**

b. **Required PHI Disclosure Accounting.** Upon request, disclosure of the following PHI shall be made to the inmate, the inmate's personal representative or a former inmate.

1) Disclosures made to the inmate or personal representative.

2) Disclosures made pursuant to the inmate's consent.

3) The PHI that was disclosed in response to a subpoena, a court order, discovery request or other lawful process not accompanied by court or administrative tribunal order, when DOC has made a reasonable effort to provide notice to the individual sufficient to permit the individual to object to, or seek a qualified protective order from, a court or administrative tribunal or there is "satisfactory assurance" that the information seeker has made reasonable efforts either (a) to ensure the individual has notice, or (b) to secure a qualified protective order from the court or administrative tribunal or by party stipulation that limits the parties' use or disclosure to the purpose of the proceeding, and requires return or destruction of the protected health information (including all copies) at end of the proceeding.

c. **Exemptions for Disclosure Accounting.** DOC shall not provide notice of PHI that falls under the realm of *Permitted Use and Disclosure* (See Chapter 5, Section 2) or when the PHI meets criteria as *Exceptions to Permitted Disclosure* (see Chapter 6).

d. **Individual's Request to DOC for an Accounting of PHI Disclosures.** The inmate, the inmate's personal representative or a former inmate shall submit to the DOC Privacy Officer a request for disclosure accounting, using *DOC – HIPAA FORM 40A* (Attachment J).

e. The DOC Privacy Officer shall access the ePartner Software and extract instances of disclosure as set forth only in ¶ b of this section.

f. The DOC Privacy Officer shall, using *DOC – HIPAA FORM 40B Disclosure Accounting* (Attachment K) provide disclosure accounting.

b. **Response to a request for disclosure accounting**

1) Inmates or their personal representative and former inmates have the right, upon request, to a list of instances in which DOC or its business associates disclosed PHI after April 13, 2003.

2) Disclosure accounting shall be made in accordance with Privacy Rules and this directive in ¶ "b." of this section.

CHAPTER 10

PHI AMENDMENTS, RESTRICTIONS AND COMPLAINTS

1. AMENDMENT TO PHI

a. A current/former inmate or the inmate's personal representative has the right to request that DOC and/or its business associates amend PHI as long as DOC maintains the record.

b. DOC has no obligation to agree to the request.

c. Only the DOC Privacy Officer, or designee, shall determine whether to grant or deny a current/former inmate's amendment request.

d. DOC shall not amend PHI if:

1) DOC or its business associates did not create the information – unless the individual can provide reasonable proof that the originator is no longer available to act on the request.

2) The information is not part of the designated record set DOC maintains.

3) The information would not be available for inspection (due to its condition or nature).

4) The information is determined to be accurate and complete.

d. If DOC is informed by another covered entity of an amendment to a current/former inmate's PHI in accordance with the provisions of the Privacy Rule, DOC shall amend the PHI in the designated record set for that inmate.

e. **PROCEDURES**

1) **Request Form.** The inmate or the inmate's personal representative shall forward the request to the DOC Privacy Officer, using *DOC-HIPAA FORM 39A Request to Amend PHI* (Attachment L).

2) **Amendment Request Processing**

a) DOC shall, at a minimum, identify the records in the designated record set that are affected by the amendment.

b) The DOC privacy Officer shall, using *DOC – HIPAA FORM 39B Amendment Request Processing* (Attachment M) forward the request for amendment to the business entity who is believed to maintain the PHI.

(1) The business entity shall review the request for amendment and, using *DOC – HIPAA FORM 39B*, submit a recommendation to the Privacy Officer.

(2) If amendment is recommended, the business partner shall prepare the specific language for amendment and submit it as an attachment to *DOC-HIPAA FORM 39B*.

3) **Granting the Amendment**

a) The DOC Privacy Officer shall document the grant of amendment on FORM 39B and in the EPartner software.

b) The DOC Privacy Officer shall, using *DOC -- HIPAA FORM 39C Grant of Amendment to Records* (Attachment N), respond in writing to the request to amend PHI within 60 days of its receipt.

c) The DOC Privacy Officer shall, using *DOC – HIPPA FORM 39D Notification to Amend Records* , (Attachment O) make reasonable efforts to inform and provide the amendment within a reasonable time to:

(1) People identified by the current/former inmate or personal representative as having received the PHI and needing the amendment.

(2) The business associates, that control the PHI and who may have relied, or could rely, on the information.

(3) The current/former inmate or personal representative must agree with the parties with whom the amendment will be shared.

(4) The DOC Privacy Officer shall inform the current/former inmate or personal representative of complaint rights if the inmate does not agree with the amendment made or with whom the amendment was shared.

f. **Denying the Amendment**

1) If a request to amend is denied, the DOC Privacy Officer shall, using *DOC – HIPAA FORM 39E Denial of Request to Amend Records*

(Attachment P), provide the current/former inmate or personal representative with a determination in a timely manner that is written in plain language, stating:

a) The basis for the denial.

b) Notification of the right to submit a written statement of disagreement and instructions for doing so.

c) Notification of the right to ask DOC to include the request for amendment, the denial and the disagreement with any future disclosures of PHI that are the substance of the amendment.

d) Procedures for filing a complaint to include the name, address and telephone number to the District Privacy Official and the Secretary of the Department of Health and Human Services.

2) If the current/former inmate or the inmate's personal representative has submitted a written statement of disagreement, DOC shall, using *DOC – HIPAA FORM 39D*, direct its business entities to, when making future disclosure of the affected PHI, include the following:

a) The request for amendment.

b) The denial.

c) The statement of disagreement.

d) The rebuttal (if any).

e) At the DOC Privacy Officer's discretion, an accurate summary of the requester's disagreement along with DOC' s rebuttal.

4) The DOC Privacy Officer shall document the actions taken in response to the amendment request on HIPAA FORM 39B and in ePartner Software.

2. **REQUEST TO RESTRICT USE AND DISCLOSURE OF PHI.** A current/former inmate or the inmate's personal representative may request DOC or the business associate to restrict use and disclosure of or the inmate's personal representative PHI for treatment, health care operations, disclosure to specified family members or others, and for other notification purposes.

a. Only the DOC Privacy Officer, or designee, may grant the current/former inmate or personal representative's request to restrict use and disclosure of PHI.

b. DOC has no obligation to agree to the request.

c. **Unenforceable Restrictions.** The DOC Privacy Officer shall not grant a restriction to disclosure as follows:

1) When the use or disclosure when the inmate's consent to disclose the PHI is not required,

2) Disclosure to the Department of Health and Human Services for compliance investigation or enforcement, or

3) When use or disclosure is for permitted public interest or benefit activities.

d. **Medical emergencies.** DOC and its business entities may use restricted PHI for treatment in a medical emergency but shall:

1) Exercise professional judgment to determine that the medical emergency justifies disclosure.

2) Document the basis for the determination.

3) Send documentation to the DOC Privacy Officer and place a copy in the inmate's medical record.

e. **Procedures**

1) **Request Form.** The requester shall submit *DOC – HIPAA FORM 42A Request to Restrict Disclosure of PHI* (Attachment Q) to the DOC Privacy Officer.

2) The DOC Privacy Officer shall, at a minimum, identify the records in the designated record set and where the records are maintained that are affected by the restriction.

3) **Agreement to the Restriction**

a) Upon agreement to the Restriction, the DOC Privacy Officer shall:

(1) Using *DOC – HIPAA FORM 42B Agreement to Restrict Disclosure of PHI* (Attachment R), notify the requester of the restriction and limitations of restriction cited in ¶c. of this Section.

(2) Using *DOC – HIPAA FORM 42C Notification of Restriction Protected Health Information* (Attachment S) notify affected agencies and business entities of their obligation to comply with the restriction.

(3) Ensure *DOC – HIPAA FORM 42C* is filed in the inmate's medical; and institutional filed when applicable; and retain a copy in the DOC Privacy Office's File.

b) Employees who are authorized to use and disclose PHI shall immediately notify the DOC Privacy Officer if they receive a request from HHS or another government agency or organization for PHI that is restricted.

c) Employees who are authorized to use and disclose PHI shall consult with the DOC Privacy Officer whenever there is any question of whether a particular use or disclosure may be contrary to the restriction agreement.

d) The DOC Privacy Officer shall document the transactions on *DOC – HIPAA FORM 42D Processing of Request to Restrict Disclosure* of PHI (Attachment T).

4) **Termination of the Restriction on Use and Disclosure of PHI.** Termination of Restriction can be made by either DOC or the inmate/ inmate's personal representative.

a) DOC may terminate a restriction agreement with or without the current/former inmate's or personal representative's concurrence by giving written notice of termination.

b) Only the DOC Privacy Officer has the authority to terminate a Restriction of Use and Disclose of PHI.

c) Termination of the Restriction can be enacted as follows:

(1) The Requester may submit a written request to the DOC Privacy Officer to lift the restrictions.

(2) The DOC Privacy Officer shall, *using DOC – HIPAA FORM 43A Notice of Termination of PHI Restriction Agreement* (Attachment U) notify the individual of the termination.

d) The DOC Privacy Officer shall, using *DOC – HIPAA FORM 43B Notice to Terminate Restriction for Use and Disclosure of PHI* (Attachment V), notify affected agencies and business entities that the restriction has been terminated.

5) **Denial of the Restriction.** If the DOC Privacy Officer denies a request to restrict use and disclosure of PHI, the DOC Privacy Officer shall, using *DOC – HIPAA FORM 42E Denial of PHI Restriction Request* (Attachment W), provide the current/former inmate or

personal representative with a determination in a timely manner that is written in plain language, stating the basis for the denial.

6) **Documentation.** The DOC Privacy Officer shall document the restriction request using *DOC -- HIPAA FORM 42D* and shall include in both the individual's and the Privacy Officer files records of each restriction request received, DOC response, each restriction agreement made, each restriction agreement terminated and any other documentation regarding compliance with respect to disclosure accounting.

3. **REQUESTS FOR CONFIDENTIAL COMMUNICATIONS.** Inmates may request that communications of PHI be made by alternative means, or at alternative locations. DOC may accommodate such reasons, if deemed reasonable and not likely to present a security and safety problem. The alternative is usually when the inmate requests to come to the infirmary to be verbally given the requested PHI rather than at sick call.

4. **COMPLAINTS**

a. **Authority.** The DOC Privacy Officer shall timely investigate and appropriately respond to each written complaint.

b. **Request Form.** The current/former inmate or the inmate's personal representative shall submit each complaint regarding compliance with the Privacy Rules and/or this directive using, *DOC -- HIPAA FORM 53A Health Information Privacy Complaint* (Attachment X).

c. **Procedures.** The DOC Privacy Officer shall process a complaint as follows:

1) Investigate the complaint, using *DOC -- HIPAA FORM 53B Complaint Investigation and Processing* (Attachment Y) to document the investigation, findings, and conclusions.

2) Using *DOC – HIPAA FORM 53C Report on Complaint* (Attachment Z), notify the complainant of the resolution of the complaint.

3) Institute appropriate action to correct the matters complained of, if corrective action is warranted.

4) Mark any portion of *DOC – HIPAA FORM 53C* that is subject to the attorney-client or attorney work product privilege as "privileged and confidential," and send the completed *DOC – HIPAA FORM 53C* to the DC Privacy Officer.

CHAPTER 11

RECORDS MAINTENANCE, RETENTION AND DISPOSAL

1. **Epartner.** The DOC Privacy Officer shall implement documentation and implementation practices that are consistent with the Privacy Policies and Procedures.

2. **Documentation.** The DOC Privacy Officer shall ensure that business entities and DOC staff, who are responsible for use and disclosure, enter required data into the ePartner software.

3. **Records Retention and Disposal.**

   a. The DOC Privacy Officer is the repository of all documents regarding privacy practices and compliance. Some of these documents are:

      1) Documentation of the designation of DOC Privacy Officer, documentation of designated record and limited data sets.

      2) Privacy Policies and Procedures.

      3) Consent to release PHI and revocations of the consent to release PHI.

      4) Requests from individuals for access, amendment, disclosure accounting, restriction or confidential communication.

      5) Complaints and any material generated as a result of investigating and resolving the compliant, if any.

      6) Documentation of when PHI has been declassified and notification to each covered entity.

      7) Documentation relating to personal representative relationships and business associate relationships.

      8) Documentation of workforce training and sanctions, mitigation plans and other administrative requirements.

   b. The DOC Privacy Officer, DOC and the affected business associate shall maintain or retain, on paper or electronically, the documentation obtained or received in connection with use or disclosures of PHI for 6 years after its creation or last effective date that it was used or disclosed. Documentation shall include:

1) Disclosure to or a request by a health care provider for treatment.

2) Use with and disclosure to an individual (or the individual's personal representative).

3) Use and disclosure pursuant to an authorization by an individual (or the individual's personal representative).

4) Disclosure to Health and Human Services for complaint investigation or compliance enforcement or review.

5) Use and disclosure required by law.

c. The DOC Privacy Officer shall maintain, retain and dispose of PHI in accordance with the Privacy Policy and DOC policy PS 2000.2 "Retention and Disposal of Department Records" (4/6/01) and subsequent Records Retention Schedule.

4. **Policy and Procedures Change Documentation**

a. The DOC Privacy Officer shall furnish to the District Privacy Official any documentation regarding changes in Privacy Policies and Procedures and corresponding changes in Privacy Practices Notices.

b. The District Privacy Official shall retain each set of the Privacy Policies and Procedures and all documentation reflecting changes in them and in the Privacy Practices Notices for 6 years after their creation or last effective date.

c. Privacy Policies and Procedures as well as all documentation pertaining to implementation of all policy and procedures contained in this directive shall retain documentation until 6 years after their creation or last effective date.

5. **Retention of Disclosure Documentation**

a. DOC and the affected business associate shall maintain or retain, on paper or electronically, the documentation obtained or received in connection with use or disclosures for public interest or benefit activities until 6 years after its creation or last effective date.

b. Documentation shall include:

6) Disclosure to or a request by a health care provider for treatment;

7) Use with and disclosure to an individual (or the individual's personal representative);

8) Use and disclosure pursuant to an authorization by an individual (or the individual's personal representative);

9) Disclosure to HHS for complaint investigation or compliance enforcement or review; and

10) Use and disclosure required by law.

CHAPTER 12

Oversight and Quality Assurance

1. **Contract Administration and Quality Assurance**

   a. The DOC Health Services Administrator shall in accordance with the contracts between the District, CCA and CCHPS and in accordance with DOC management controls guidelines conduct regular monitoring and oversight of agency compliance with this directive.

   b. The DOC Privacy Officer shall conduct regular monitoring activities for compliance with this directive.

   c. The Office of Internal Controls, Compliance and Accreditation shall conduct annual audits of DOC compliance with HIPAA, related laws, standards, regulations and this directive.

2. **Department of Health and Human Services (HHS) Enforcement and Compliance**

   a. Officials and employees shall immediately notify the DOC Privacy Officer of any inquiry from HHS or any other government official and shall await instruction from the DOC Privacy Officer before responding to these inquiries or providing any documents or other information on behalf of the organization.

   b. The DOC Privacy Officer, shall coordinate responses to any HHS compliance review, complaint investigation or other inquiry, to ensure that all applicable obligations of the organization are fulfilled and all applicable rights and privileges of the organization are preserved and protected.

   c. The DOC Privacy Officer shall keep sufficient non-privileged records of the compliance to be able to submit compliance reports in the time, manner, and with the information HHS requests to ascertain compliance.

   d. The DOC Privacy Officer, shall arrange for HHS to have access to facilities, books, records, accounts, and other non-privileged information.

   e. The DOC Privacy Officer, shall endeavor to obtain non-privileged information required by HHS that is in the exclusive possession of the business associates, other agents, institutions or persons who fail or refuse to furnish the information directly to HHS.

   f. No DOC official or employee shall attempt to or obstruct or interfere with any lawful process, warrant, order or subpoena that may be presented.

g. If the officials insist they have the right of immediate search and seizure of the organization's records, equipment or other matters specified in the process presented, no DOC employee or covered entity shall obstruct or interfere with them. Instead, the affected employee shall use best efforts to contact the DOC Privacy Officer or General Counsel and in the interim, observe and document everything that the officials search, seize, say, and do.

CHAPTER 13

DEFINITIONS

1. **Agency.** The DOC designated as a *health care component* in the District's *hybrid entity* declaration on file in the Privacy Officer's office.

2. **Attorney-of-record.** Disclosure to an inmate's attorney shall be handled as would all disclosures to a third party with the inmate's written consent.

3. **Covered Entity.** A health care provider who transmits any health information in electronic form in connection with a transaction covered by this directive. A *Health care provider* a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal conduct of business. The Center For Correctional Health and Policy Studies (CCHPS) is the *covered entity* contracted by the DOC to provide health care services to inmates confined within the DOC.

4. **De-identified Information.** Under certain circumstances, all identifiers of the individual and the individual's relatives, household members, and employers, associated with the health information may be removed so that the information can be used for research or statistical reporting without there being the ability to identify the individual.

5. **Designated Record Set.** For the purposes of this directive, the term *record* means any item, collection or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. A designated record set is a group of records maintained by or for a covered entity that is (1) medical and medical billing records about individuals maintained or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case of medical management record systems maintained by or for a health plan; or (3) used in whole or in part, by or for the covered entity to make decisions about individuals. Designated records sets are listed in Attachment A of this directive.

6. **Disclosure.** The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

7. **Health Care.** Care, services, or supplies related to the health of an individual, to include, but is not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an

individual or that affects the structure or function of the body; and dispensing of a drug, device, equipment, or other item in accordance with a prescription.

8. **Health Care Clearinghouse.** A public or private entity, including a billing service, re-pricing company, or health management service that processes or facilitates the processing of health information. The Department of Health (DOH) provides health care clearinghouse services for the DOC.

9. **Health Oversight Agency** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

10. **Hybrid Entity.** A hybrid entity is an entity whose covered functions are not its primary function therefore compliance with HIPAA Privacy Rules for protected health information is a hybrid entity's primary concern. DOC as a hybrid entity shall ensure the health care provider, as a covered entity, complies with all aspects of HIPAA to include privacy rules, individual identifiers, electronic transactions, payments, etc.

11. **Individually Identifiable Information.** Anything that can be used to identify a patient such as names, addresses, dates of birth, relative's names, employers, telephone numbers, e-mail addresses, social security numbers, medical record number, DCDC numbers, fingerprints, photographs, codes or other characteristics that may identify the individual.

12. **Law Enforcement Official.** An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

13. **Minimum Necessary** means to request only and to give or supply to the requester only the PHI that is required to fulfill the requester's inquiry. Do not give or supply more than is necessary to fulfill that particular inquiry.

14. **Personal Representative**. For the purposes of this directive, a personal representative is defined as an individual with a power of attorney or an individual appointed by the court or otherwise has legal authority to act on behalf of an

inmate when medical decisions must be made. *The inmate's attorney is not defined as a personal representative.*

15. **Protected Health Information.** Information regarding a person's past, present, or future physical or mental condition, provision of health care or payment for health care.

16. **Psychotherapy Notes** are personal notes as mental health information disclosed to the mental health professional in confidence by other persons on condition that such information is not disclosed to the individual or other persons; and the mental health professional's speculations.

17. **Record.** Any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

18. **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.

19. **Transaction** means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

    a. Health care claims or equivalent encounter information.

    b. Health care payment and remittance advice.

    c. Coordination of benefits.

    d. Health care claim status.

    e. Enrollment and de-enrollment in a health plan.

    f. Eligibility for a health plan.

    g. Health plan premium payments.

    h. Referral certification and authorization.

i. First report of injury.

j. Health claims attachments.

k. Other transactions that the Secretary may prescribe by regulation.

20. **Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

21. **Use.** 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.

22. **Workforce.** Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.