



DISTRICT OF COLUMBIA
DEPARTMENT OF CORRECTIONS

PROGRAM MANUAL

EFFECTIVE DATE:	January 18, 2018	Page 1 of 43
SUPERSEDES:	1300.3 December 15, 2003	
OPI:	FOIA	
REVIEW DATE:	January 18, 2019	
Approving Authority	Quincy L. Booth Director	

SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)
NUMBER:	1300.3A
Attachments:	Attachment 1 – Designated Record Sets Attachment 2 – Access to Application

SUMMARY OF CHANGES:Section	Change

APPROVED:

Signature on File



Quincy L. Booth, Director

1/18/2018
Date Signed

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 3 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

1. **PURPOSE AND SCOPE.** To provide uniform guidelines for the implementation of the District of Columbia Health Information Privacy and Security Policies, and the Security and Privacy Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health (HITECH Act) and its Final Rules.

2. **POLICY.** It is the policy of the D.C. Department of Corrections (DOC) to ensure that the DOC is in full compliance with HIPAA by seeking to maintain the confidentiality and security of individual’s health information while also seeking to meet the needs of health care industry to more efficiently process healthcare claims and certain other related transactions. To this end, DOC shall provide guidelines 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.** The policy applies to DOC employees, contractors, volunteers, visitors and inmates as well as to DOC business associates and their employees.

4. **NOTICE OF NON-DISCRIMINATION**
 - a. In accordance with the D.C. Human Rights Act of 1977, as amended, D.C. Official Code § 2-1401.01 et seq., (hereinafter, “the 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, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, 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.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 4 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

5. PROGRAM OBJECTIVES

- a. To ensure the confidentiality, integrity, and authorized availability of all protected health information that DOC creates, receives, maintains or transmits.
- b. To protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- c. To protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA.
- d. Protected health information shall be used, stored and disclosed in accordance with HIPAA Privacy and Security Rules as implemented in this directive.
- e. All employees shall receive appropriate training in what constitutes protected health information and guidance to ensure appropriate use and disclosure of PHI.
- f. 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 and recorded on the DOC Designated Record Set form (Attachment 1).

6. DIRECTIVES AFFECTED

- a. **Directives Rescinded**
 - 1) PM 1300.3 Health Information Privacy (HIPAA) (12/15/03)

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 5 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

b. **Directives Referenced**

- 1) PP 2420.4D Email and Internet Use
- 2) SOP 2420.8-17 Disaster Recovery Plan

7. AUTHORITY

- a. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936, 45 C.F.R. Parts 160, 162 & 164.
- b. Health Information Technology for Economic and Clinical Health Act (HITECH Act), 42 USC §17921 et seq.
- c. D.C. Code §7-242 (Use and disclosure of health and human services information.)
- d. D.C. Code §7-1605; §22-3903 (Confidentiality of medical records and information.)
- e. D.C. Code §7-1201 et seq. (Confidentiality of mental health information.)
- f. 42 U.S.C. §290dd-2 (Confidentiality of substance abuse treatment records.)

8. STANDARDS REFERENCED. American Correctional Association 4th Edition Performance Based Standards for Adult Local Detention Facilities: 4-ALDF-4D-14

9. EXCLUSIONS

- a. **Employment Records.** Health information in employment records held by DOC in its role as employer is not subject to this policy. DOC shall continue to use and disclose DOC employee records in accordance with DPM Chapter

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 6 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

31A “Records management and privacy of Records” and other applicable regulations, policy and procedure.

- b. **Educational Records.** Educational records are subject to the protection of the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g.
- c. **Security Restrictions for Inmates.** Inmates shall be given the opportunity to inspect their PHI unless a determination is made, on a case-by-case basis, that the safety of inmates or staff may thereby be jeopardized.
- d. **Copy Restrictions for inmates.** Inmates shall not be permitted to keep with them a copy of their PHI while they are in the custody of the DOC, because to do so would not ensure appropriate physical safeguards of the documents and may jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety security or order of the facility or staff persons.
- e. **Privacy Practices Notice.** HIPAA excludes Correctional/Jail facilities from privacy Practices Notice requirement.
- f. **Psychotherapy Notes.** Clinician’s personal (psychotherapy) 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, these notes must be maintained separately from an individual’s official record of mental health information so as to avoid incidental disclosure in connection with an otherwise valid disclosure of the records.

10. DEFINITIONS

- a. **Access.** To inspect and/or obtain a copy of protected health information. As additionally applied to electronic protected health information, ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 7 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- b. **Administrative Safeguards.** Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.
- c. **Agency.** The D.C. Department of Corrections (DOC), designated as a health care component of the District of Columbia, a hybrid entity.
- d. **Authorization.** A document signed and dated by an individual (or his representative) who authorizes use and disclosure of the individual’s protected health information for a stated reason other than treatment, payment or health care operations. An authorization must, at a minimum, further contain a description of the protected health information, the names or class or persons permitted to make a disclosure, the names or class of persons to whom the covered entity may disclose, an expiration date or event, an explanation of the individual’s right to revoke and how to revoke and a statement about potential re-disclosures.
- e. **Breach.** The unauthorized acquisition, access, use, or disclosure of PHI in a manner which compromises the security or privacy of the PHI, except where an unauthorized person to whom the PHI is disclosed would not reasonably have been able to retain the PHI.
- f. **Business Associate (BA).** A person or entity which , on behalf of DOC/District government, creates, receives, maintains or transmits protected health information for a function or activity for the DOC/District government, including claims processing or administration, data analysis, processing or administration. A **subcontractor** that does the same on behalf of a BA is equally subject to the HIPAA business associate provisions. BA may include Patient Safety Organizations, Health Information Organizations, E-Prescribing Gateways, protected health information data transmission service providers with routine access to protected health information and vendors of personal health records with access to protected health information that offer access to individuals on behalf of covered entities.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 8 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- g. **Business Associate Agreement.** A contract between a covered entity and a business associate that 1) establishes the permitted and required uses and disclosures of PHI by the business associate, 2) provides that the business associate will use PHI only as permitted by the contract or as required by law, use appropriate safeguards, report any disclosures not permitted by the contract, ensure that agents to whom it provides PHI will abide by the same restrictions and conditions, make PHI available to individuals and make its record available to US Department of Health and Human Services, 3) authorizes termination of the contract by the Department if the Department determines that there has been a violation of the contract.
- h. **Covered Entity.** A health plan, health care clearinghouse or a health care provider who electronically transmits any covered transactions.
- i. **Covered Component.** DOC: a designee of a Covered Entity.
- j. **Designated Record Set.** A group of records maintained by or for a covered entity that maintain the medical records and billing records about individuals maintained by or for a covered health care provider, b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, or c) used, in whole or in part, by or for the covered entity to make decisions about individuals. (Attachment 1).
- k. **Disclosure:** Release, transfer, provision of access to, or divulging of PHI outside of DOC.
- l. **Encryption.** The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- m. **Hybrid entity.** District of Columbia: a single legal entity which is a covered entity, whose business activities include both covered and non-covered functions and designates health care components.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 9 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- n. **Individual.** The person who is the subject of PHI.
- o. **Information System.** An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.
- p. **Integrity.** The property that data or information have not been altered or destroyed in an unauthorized manner.
- q. **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, or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- r. **Malicious software or malware.** Software, such as a virus, designed to damage or disrupt a system.
- s. **Office of Civil Rights (OCR).** The Office for Civil Rights, that part of the US Department of Health and Human Services responsible for enforcing HIPAA's Privacy and Security Rules.
- t. **Psychotherapy notes.** Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 10 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- u. **Protected Health Information/Electronic (PHI & EPHI).** Health information that a covered entity [or covered component] creates or receives that identifies an individual and relate to past, present, or future physical or mental health or condition, which may be 1) oral (e.g., clinical conversation at nursing station, physician-family or physician-patient conversation at bedside), 2) written/printed (e.g., medical record, surgery schedule, billing statement, insurance claims, driver’s license) and 3) electronic (e.g., electronic claim, digitally stored z-ray images, clinical photograph, patient information sent via text or email).

- v. **Public health authority.** 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 responsible for public health matters as part of its official mandate.

- w. **Physical safeguard.** Physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

- x. **Required by law.** 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, which includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grant 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.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 11 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
		SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)	
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- y. **Technical Safeguard.** The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

- z. **TPO.** Treatment, payment and [health care] operations, three categories of uses and disclosures that Covered Entities can generally make without a patient authorization.

- aa. **Use.** The sharing, employment, application, utilization, examination, or analysis of PHI within DOC.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 12 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

TABLE OF CONTENTS

	Purpose and Scope	Page 2
	Policy	Page 2
	Applicability	Page 2
	Notice of Non-Discrimination	Page 2
	Program Objectives	Page 3
	Directives Affected and Referenced	Page 3
	Authority	Page 4
	Standards Referenced	Page 4
	Exclusions	Page 4
	Definitions	Page 4-10
	Table of Contents	Page 11-13
	Introduction	Page 14
Chapter 1	<i>Privacy Rule</i>	Page 16
	Access to PHI	Page 16
	Amendments of PHI	Page 16
	Accountings of Disclosures	Page 17
	Individual's Rights to Restrictions of Uses and Disclosures	Page 17
Chapter 2	<i>Complaints about Uses & Disclosures of PHI</i>	Page 19
Chapter 3	<i>Security Rule</i>	Page 20
	Administrative Safeguards	Page 20

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 13 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

Sanctions	Page 20
Security Responsibility	Page 20
Information System	Page 20
Workforce Security/Clearance	Page 22
Authorization and/or Supervision	Page 23
Employee Separation	Page 24
Security Monitoring and Protection	Page 25
Reporting of, and Response to Security Incidents	Page 25
Contingency/Disaster Plan	Page 26
Data Backup Plan	Page 26
Disaster Recovery Plan	Page 26
Emergency Mode	Page 27
Testing and Revision	Page 27
Application and Data Criticality Analysis	Page 27
Periodic & Triggered Evaluations Policy	Page 29
Business Associates and Agreements	Page 30
Physical Safeguards	Page 30
Facility Security Plan	Page 30
Facility Contingency Plan	Page 31
Facility Maintenance Records	Page 31
Workstation Use and Security	Page 32

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 14 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
		SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)	
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

Device and Media Protection	Page 32
Technical Safeguards	Page 34
Unique User and Password	Page 34
Emergency Access Procedure	Page 35
Automatic Logoff	Page 36
Acceptable Encryption	Page 36
Audit Controls	Page 37
Data Integrity	Page 38
Persons or Entity Authentication	Page 39

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 15 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

INTRODUCTION

The health Insurance Portability and Accountability Act of 1996 (HIPAA), passed by Congress and signed into law in 1996, went into effect on July 1, 1997. Its privacy rules established standards for the protection, privacy, security, disclosure and non-disclosure of health information about individuals. Requirement to comply with the HIPAA privacy rules (“privacy Standards”) came into force on April 14, 2003. There are also the HIPAA security regulations, which established standards for ensuring the integrity, confidentiality and availability of electronically managed health information. Final HIPAA security regulations were published on February 20, 2005. Most recently, the American recovery and Reinvestment Act of 2009 became law on February 17, 2009, part of which is the Health information Technology for Economic and Clinical Health Act (the HITECH Act). The HITECH Act both expands the HIPAA Privacy and Security Rules and increases the penalties for violations of HIPAA.

DOC is a component of a covered “hybrid” entity (the District of Columbia government), which provides the following services to its inmate population through business associates: health care (Unity health Care, Inc.), food service (ARAMARK), and security (Corrections Corporation of America (CCA)). Under HIPAA Privacy Rules, DOC, CCA/CTF and ARAMARK shall respectively ensure that appropriate administrative, technical and physical safeguards are in place to protect the privacy of protected health information about inmates and employees. DOC, CCA/CTF and ARAMARK shall maintain policies, procedures and practices to enforce HIPAA privacy rules.

Only designated employees with particular job functions are authorized to **use** and **disclose** protected health information. Each member of the District’s work-force, 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.

1. **DOC Privacy Officer Roles and Responsibility.** The Privacy Officer is responsible for:
 - a. Understanding the HIPAA Privacy Rule and how it applies within the D.C. Department of Corrections (DOC).

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 16 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
		SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)	
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- b. Developing policies and procedures for the implementation of the HIPAA Privacy Rule, and monitoring compliance with the policies and procedures.
- c. Overseeing the enforcement of inmates' privacy rights as granted by the HIPAA Privacy Rule.
- d. Developing and implementing HIPAA privacy training for employees of the DOC.
- e. Notifying the HIPAA Security Officer of a Business Associate Agreement that implicates EPHI prior to the effective date of the agreement.
- f. Receiving and responding to complaints of alleged non-compliance with HIPPA Privacy Rule.

2. HIPAA Security Officer Roles and Responsibility. The HIPAA Security Officer shall be responsible for understanding the HIPAA Security Rule and how it applies within the DOC, and, in collaboration with the Privacy Officer, his duties shall include:

- a. The development of policies and procedures for the implementation of the HIPAA Security Rule, and monitoring compliance with the policies and procedures.
- b. Overseeing the security of EPHI maintained by DOC.
- c. Periodic assessments to determine any need for agency Security policy modifications.
- d. Responding to actual or suspected breaches in the confidentiality or integrity of EPHI.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 17 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

CHAPTER 1

PRIVACY RULE

1. INMATE ACCESS TO PHI

- a. All access requests shall be forwarded to the DOC Privacy Officer, who will provide a response.
- b. Inmates in the custody of the DOC shall not keep a copy of their medical records with them during the period of their incarceration because to do so would not ensure appropriate physical safeguards of the documents and may jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety security or order of the facility or staff persons. They may, however, authorize disclosure of the records to a third party outside the agency.
- c. The cost of copying the records shall be 25 cents per page, chargeable to the requester.
- d. If an access request is denied, notice of denial shall include: a) basis for denial, b) procedure by which the requester may appeal the denial, and c) the procedure by which the patient may file a complaint with the Secretary of HHS.

2. AMENDMENTS OF PHI

- a. All requests for an amendment of PHI shall be written and addressed to the DOC Privacy Officer, to include reason(s) justifying amendment and an authorization that identifies parties that should be notified of the amendment.
- b. A final decision on the request shall be made within 60 days of the request.
- c. If the request is granted, the DOC Privacy Officer shall promptly notify the requester and the parties identified in the request.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 18 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- d. If the request is denied, the DOC Privacy Officer shall notify the requester in writing, stating a) the basis for the denial, and b) requester’s right of appeal and/or complaint to the Secretary of HHS.

3. ACCOUNTINGS OF DISCLOSURES

- a. A request for accounting shall be written and addressed to the DOC Privacy Officer who shall provide a response within 60 days of receipt.
- b. Accounting shall cover disclosures made within 6 years of the date request for accounting was received.
- c. Accounting shall not include disclosures that the Privacy Rule does not require to be documented.
- d. An accounting shall include a) date of disclosure, b) name and, if know, the address of the person or entity to whom the disclosure was made, c) description of the PHI disclosed, and d) purpose for the disclosure.
- e. DOC Privacy Officer shall suspend the right to an accounting if the agency has received a documented notice from a health oversight committee or a law enforcement agency that making an accounting would impede such agency’s activities.
- f. A written record of suspension of right to an accounting shall be maintained along with the individual’s medical records.

4. RIGHT OF AN INDIVIDUAL (INMATE) TO REQUEST RESTRICTIONS OF USES AND DISCLOSURES

- a. A request for restrictions of uses and disclosures shall be written and addressed to the DOC Privacy Officer, who shall provide a response.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 19 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
		SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)	
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- b. If the request is granted, the DOC Privacy Officer shall provide a written notice of the grant to the requester and a copy of the notice, together with the written request, shall be maintained along with the individual’s medical records.
- c. A grant of uses and disclosures restriction does not apply to emergency treatment need.

5. DATA SHARING

- a. Data shall be collected and shared on the basis of privacy, security, transparency, legal conformity, data protection and accountability considerations.
- b. Any data sharing proposal, either by agreement or other means, shall be reviewed for HIPAA conformance by the Privacy Officer and the General Counsel prior to execution.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 20 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

CHAPTER 2

INMATE COMPLAINTS ABOUT USES & DISCLOSURES OF PHI

1. An inmate complaint about uses and disclosures of PHI shall be written and addressed to the DOC Privacy Officer, and question about filing a privacy complaint with the agency or with the Health and Human Services (HHS) Secretary may be directed to the DOC Privacy Officer.
2. The DOC Privacy Officer shall log the complaint, noting receipt date, substance of the complaint and other pertinent information.
3. The DOC Privacy Officer shall investigate the complaint and produce an investigation report and, in collaboration with the DOC Office of Human Resource, determine appropriate sanction, if found that violation occurred.
4. Once the investigation has been completed and closed, the DOC Privacy Officer shall provide a written notice of the investigation outcome to the complainant.
5. Retaliation against a complainant or anyone that assisted in the filing the complaint is prohibited.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 21 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

CHAPTER 3

SECURITY RULE

1. **ADMINISTRATIVE SAFEGUARD.** To ensure appropriate administrative safeguard, the procedures below shall be followed.
 - a. **SANCTION**
 - 1) All violations of DOC’s Electronic Protected Health Information Database shall be subject to disciplinary action.
 - 2) Action may range from verbal warnings to termination and referral for criminal prosecution, depending on the nature and circumstances of the violation.
 - 3) All employees that are given access also assume the responsibility to be familiar with the HIPAA policy.

2. **HIPAA SECURITY OFFICER’S RESPONSIBILITY**
 - a. The Chief of the Office of Information Technology (IT) shall serve as HIPAA Security Officer and, in collaboration with the Privacy Officer, develop as well as implement HIPAA security guidelines, which shall include:
 - 1) Training of employees on the purpose and requirements of the HIPAA policy and Security Rule.
 - 2) Periodic assessments to determine any need for agency HIPAA policy modifications.

3. **INFORMATION SYSTEM**
 - a. The HIPAA Security Officer or designee shall:

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 22 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 1) Ensure that all systems applications involving ePHI are monitored and routinely reviewed for overall compliance purposes to discourage, detect, and/or prevent security violations. (Attachment 2)
- 2) Identify, investigate, report, document, and respond to all suspicious events and/or inappropriate activity.
- 3) Ensure that all audit logs from systems application concerning ePHI will capture information and events which may include:
 - a) Machine startup and shutdown.
 - b) Successful/unsuccessful login and logout of users.
 - c) Add, modify, or delete actions on all data files.
 - d) Use of all privileged accounts and utilities.
 - e) Changes to user accounts or privileges.
 - f) Automatic logout of a user after exceeding a locally defined time of inactivity or excessive login attempts.
 - g) Software or hardware modification.
 - h) All access to security files, attributes, and/or parameters.
 - i) Detection of a virus.
 - j) Changes to log files.
 - k) Detectable hardware and software errors.
 - l) Network ling failures.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 23 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- m) Overrides of network abnormality alarms and alerts, and
 - n) Changes to network security configuration.
- 4) Develop audit logs shall contain:
- a) Date
 - b) Time
 - c) Any applicable error
 - d) The user identification of the person who caused the event
 - e) The application(s) that created the audit event
 - f) The application(s) responsible for executing the event
 - g) The DOC Workstation that initiated the event and the location thereof, and
 - h) A detailed description of the event.
- 5) Conduct monitoring and review process, which shall include an audit of system activity and the associated reports at a level commensurate with the criticality of the systems application in question.
- 6) Retain any and all documentation pertaining to the review of audit logs for six (6) years.

4. WORKFORCE SECURITY/CLEARANCE

- a. All employees must be adequately screened during hiring process.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 24 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- b. The screening process may include character references, professional license validation, criminal background check and/or confirmation of academic and/or professional qualifications.
- c. The type of screening performed shall be determined by DOC Human Resource Management (DOC HR) personnel based upon a risk analysis relevant to the level of access being authorized.
- d. When defining a position, DOC HR personnel must identify the security responsibilities and supervision required for the position.

5. AUTHORIZATION AND/OR SUPERVISION

- a. Only authorized employees, and those who have a need to know because of their job assignments, shall have access to PHI.
- b. Each manager shall ensure that employees within his or her purview receive training in:
 - 1) Appropriate use of PHI access rights, inclusive of password management.
 - 2) Level of PHI access required to perform the essential functions for the job
 - 3) Authenticating into the system
 - 4) Level of access authorized and granted to employee including any modifications thereto, and/or the termination thereof, shall be routinely documented.
 - 5) Access must be promptly modified or terminated consistent with the minimum level necessary for the individual to complete his or her job duties. Action taken must be documented.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 25 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 6) Any potential violation of this policy shall be promptly reported to the Security Officer, who shall, without delay, take actions to remedy and mitigate.

6. EMPLOYEE SEPARATION

- a. Upon separation from the agency, an employee's access, including remote access, to all agency information systems, networks, system applications, and/or physical locations which contain PHI shall be immediately terminated. If the separation is by termination or a separation other than the employee's willing resignation, the revocation of access right shall be effected prior to the employee's notification of the separation. (Attachment 2).
- b. Security Officer or designee shall document separation to ensure that:
- 1) Portable computers, peripherals, and/or files were collected
 - 2) Keys, tokens and/or cards that allow physical or information systems access were collected
 - 3) The former employee has been removed from access lists and/or global email lists
 - 4) Any and all user accounts for the former employee have been removed from the information system(s), and
 - 5) Physical locks and/or keys, if necessary, have been changed.
- c. Within 1 business day of the separation, the Security Officer or designee shall confirm all physical and systems access to PHI has been revoked, disabled, and/or removed through the appropriate test procedures.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 26 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- d. Records documenting the termination processing outlined in this policy shall be maintained for a minimum of six (6) years.

7. SECURITY MONITORING AND PROTECTION

- a. Employees whose job duties could potentially require access to PHI must receive training in awareness of HIPAA, to include: risk areas, access granting and revocation procedures, access levels, password management, virus protection, identifying and reporting security breaches, and associated disciplinary procedures.
- b. Passwords are required and must be changed routinely and as outlined in the DC Government/OCTO Web Mail programs. Employees shall maintain their passwords confidentially in accordance with PP 2420.4, "Email and Internet Use".
- c. All system users must report any suspicious activity, such as sharing confidential agency data and using systems in a way that is not compliant with security procedures.

8. REPORTING OF, AND RESPONSE TO SECURITY INCIDENTS

- a. If a security incident occurred, each employee that was involved in, or witnessed the incident shall submit a written report of the incident to both the Privacy Officer and the Security Officer. The Security Officer shall take appropriate steps to resolve the incident.
- b. A log of security incidents shall be maintained by the Security Officer, to include:
 - 1) A detailed description of the security incident
 - 2) Time and date reported

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 27 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 3) Time and date of the occurrence
 - 4) The name of the individual who reported the incident, and
 - 5) The employee assigned to resolve the incident.
- c. The Security Officer shall maintain records of security incidents for a minimum of six (6) years.

9. CONTINGENCY/DISASTER PLAN

- a. *DATA BACKUP PLAN.* The Office of Information Technology (IT) shall maintain servers in the Computer Room and perform local and remote backup each night on key servers. IT shall conduct daily review of backup logs to ensure successful operations were performed in accordance with SOP 2420.8, "Disaster Recovery Plan". The following procedures shall be followed when backing up data:
- 1) All ePHI shall be stored on network servers in order for it to be automatically backed up by the system.
 - 2) ePHI shall not be saved on the local C-drive of any workstation.
 - 3) ePHI stored on portable media shall be saved to the network to ensure backup of the ePHI.
 - 4) The Data Backup shall apply to all files that may contain ePHI.
 - 5) Data Backup shall be tested on at least an annual basis to ensure the exact copies of ePHI can be retrieved and made available.
- b. *DISASTER RECOVERY PLAN.* The Department of Corrections shall ensure routine backup and disaster recovery and continuity of operations.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 28 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

ePHI application, files and data shall be backed up regularly in accordance with SOP 2420.8 to enable recovery in the event of disaster or other disruption of computing services.

- c. *MASS MEDIA COVERAGE.* The DOC Office of Government and Public Affairs (OGPA) shall coordinate requests for information regarding the release of official government information. Any dissemination of information such as HIPPA, access to medical, mental health shall be approved by the FOIA Officer and OGPA. HIPPA information is protected and privileged.

10. EMERGENCY MODE

- a. The Security Officer shall set up an emergency mode operation plan, outlining the procedure to follow in order to protect the security of ePHI during and immediately after a crisis.
- b. The procedure shall be tested periodically.

11. TESTING AND REVISION

- a. Testing procedures shall be developed for the data backup, disaster recovery, and emergency mode operations plan, and the testing must be conducted on a periodic basis to ensure that critical business processes can continue in a satisfactory manner even if primary delivery method is unavailable at a particular time.
- b. The Security Officer shall ensure that each system that collects, maintains, uses, or transmits ePHI has a documented testing and revision plan.

12. APPLICATION AND DATA CRITICALITY ANALYSIS

- a. In the event of a disaster or emergency, criticality analysis shall be done as a basis of disaster recovery plan for the recovery prioritization of ePHI and ePHI systems.
- b. Critical areas of the business that must be assessed include:

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 29 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 1) Critical business functions
 - 2) Critical infrastructure
 - 3) Critical ePHI or records
- c. The specific components of applications and data criticality analysis must include:
- 1) Network architecture diagrams and system flowcharts that show current structure, equipment addresses, communication providers and system interdependencies
 - 2) Identification and analysis of key applications and systems used to support critical business processes.
 - 3) A prioritized list of key applications and systems and their recovery time objectives.
 - 4) Documented results of an analysis of the internal and external interfaces with key applications and systems.
 - 5) Adequate redundancies within the network infrastructures to reduce or eliminate single points of failure.
 - 6) Mitigating controls or work-around procedures in place and tested for single points of failure that are unable to be eliminated.
- d. Criticality of specific applications and data relative to each area where PHI is stored shall be assessed for the purpose of developing data backup plan, disaster recovery plan and emergency mode operation plan. This shall be done periodically, at least annually, to ensure that appropriate procedures are in place for data and applications at each level of risk.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 30 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

13. PERIODIC & TRIGGERED EVALUATIONS REQUIREMENTS

- a. DOC shall undertake periodic evaluations of its security safeguards to determine the extent of compliance with the standards implemented under the HIPAA Security Rule. In addition, an evaluation shall specifically be undertaken if there is an environmental or operational change that could impact the confidentiality, integrity, and/or availability of ePHI, such as:
 - 1) Known security incidents or breaches
 - 2) Significant new threats or risks to the security of ePHI
 - 3) Changes to DOC's organizational or technical infrastructure
 - 4) Changes to information security requirements or responsibilities, and
 - 5) New security technologies that are available and new security recommendations.
 - 6) The evaluation shall be conducted by the Security Officer or designee, and/or certified by a third party.

- b. An evaluation shall include reasonable and appropriate activities, such as:
 - 1) A review of DOC's HIPPA to evaluate its appropriateness and efficacy in protecting against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability or ePHI.
 - 2) A gap analysis to compare DOC's HIPPA policy against actual practices.
 - 3) An identification of current and/or potential threats and risks to ePHI and ePHI Systems.
 - 4) An assessment of DOC's security controls and processes as reasonable and appropriate protections against the risks identified for ePHI Systems.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 31 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 5) Testing and evaluation of DOC’s security controls and processes to determine whether such has been implemented properly and whether those controls and processes appropriately protect ePHI. An authorized workforce member shall be designated to conduct the testing.
- c. The evaluation process and outcome shall be documented and the report maintained by the Security Officer.
- d. If warranted by the result of the evaluation, HIPAA security policy shall be updated.

14. BUSINESS ASSOCIATES AND AGREEMENTS

- a. The General Counsel shall determine the legal sufficiency of the HIPAA Clause to be inserted in all DOC’s Business Associates Agreements (BAA) and Memorandum of Understanding (MOU).
- b. The DOC Privacy Officer shall have access to the database of all BAA/MOU and determine which should have HIPAA Clause inserted into them.
- c. ***Physical Safeguards***
 - 1) **Facility Security Plan**
 - a) DOC shall safeguard facilities and equipment containing its PHI against unauthorized physical access, tampering and theft, and periodic auditing shall be conducted to ensure that safeguards are continuously maintained.
 - b) Each such facility shall be locked at all times, and accessible by computerized keypad only to employees with need of access and with access code.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 32 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

15. FACILITY CONTINGENCY OPERATIONS

- a. Each facility that contains ePHI shall have emergency access procedures in place that allow facility access for appropriate workforce members to access ePHI as well as support restoration of lost ePHI.
- b. The workforce members with emergency access shall include a primary contact person and back-up person when facility access is necessary after business hours by persons who do not currently have access to the facility outside of regular business hours.

16. FACILITY ACCESS CONTROLS AND VALIDATION PROCEDURES

- a. No one shall gain physical or system access to agency's information system resources without an authorization.
- b. The Security Officer shall maintain a record of all physical or system access authorizations.
- c. All system users, including technical maintenance personnel, shall receive system security awareness training.
- d. All end user personnel shall sign an End User Policy Notification Form.
- e. The Security Officer shall periodically review PHI access levels granted to each end user and process access termination as necessary.

17. FACILITY MAINTENANCE RECORDS

- a. Repairs or modifications to the physical building for each facility where ePHI can be accessed shall be logged and tracked.
- b. The log shall include at a minimum events that are related to security (for example, repairs or modifications of hardware, walls, doors, and locks).

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 33 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

18. WORKSTATION USE AND SECURITY

- a. All workstations used by workforce members to access ePHI shall be set to automatically lock the computer when it is left unattended, necessitating the user to enter a password to unlock the workstation.
- b. The standard setting for the computer to lock after a period of inactivity is not to exceed 15 minutes, with a recommended inactivity timeout of 5 minutes.
- c. ePHI Users shall:
 - 1) Manually lock their workstation computer using the Ctrl-Alt-Delete-Enter keys when the computer is left unattended for any period of time.
 - 2) Ensure that observable confidential information is adequately shielded from unauthorized disclosure and access on computer screens.
 - 3) Protect printed versions of ePHI that have been transmitted via fax or multi-use machines by promptly removing documents from shared devices.

19. DEVICE AND MEDIA PROTECTION

DOC shall protect all hardware and electronic media that contain ePHI. These electronic media include: computers, laptops, personal digital assistants (PDAs), such as Blackberry's, and smartphones, USB drives, backup tapes, CDs, flash drives and memory keys/cards.

- a. Portable Media Security
 - 1) DOC shall protect all hardware and electronic media that contain ePHI. These electronic media include: computers, laptops, personal digital assistants (PDAs), such as Blackberry's and smartphones, USB drives, backup tapes, CDs, flash drives and memory keys/cards.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 34 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
		SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)	
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 2) ePHI that is contained in portable electronic media shall be encrypted so that access to the ePHI can only be attained by authorized individuals with knowledge of the decryption code.
 - 3) Workforce members shall limit the quantity of ePHI on portable electronic media to the minimum necessary for the performance of their duties.
 - 4) All workforce members shall receive permission from their supervisor before transporting ePHI outside of the secured physical perimeter of the DOC facilities.
 - 5) Portable media that contain ePHI shall not be left visible in vehicles or any other unsecured location.
 - 6) Loss of portable media shall immediately be reported to a supervisor and/or the Security Officer.
- b. Electronic Media Disposal: Prior to disposition,
- 1) Hard drives shall be either wiped clean by IT or destroyed to prevent recognition or reconstruction of the information, and the hard drive tested to ensure the information cannot be retrieved.
 - 2) PDAs shall have all stored ePHI erased or shall be physically destroyed.
 - 3) Storage media, such as backup tapes, USB flash drives and CDs, shall be physically destroyed (broken into pieces) before disposing of the item.
- c. Electronic Media Reuse
- 1) All ePHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the ePHI, and hard drives shall be wiped clean by IT before transfer.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 35 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 2) All other media shall have all the ePHI removed and tested to ensure the ePHI cannot be retrieved. If the media is not “technology capable” of being cleaned, the media shall be overwritten or destroyed.

- d. Device Maintenance and Repair. All ePHI shall be removed from hard drive and the memory of devices (computer servers, copiers, printers and other devices capable of storing electronic data) before maintenance or repair service.

- e. Device and Media Acquisition. Security requirements and/or security specifications shall be included in information system acquisition contracts.

- f. **Technical Safeguards**
 - 1) **Unique User ID and Password - ePHI**
 - a) *User ID*
 - 1) Each authorized user shall be assigned a unique user ID that identifies the individual employee or third party.
 - 2) The unique user ID shall permit activities performed on the DOC network, systems and applications to be traced to the individual employee or third party.
 - 3) The authorized user shall not share his/her unique user ID with other individuals.
 - 4) In circumstances where there is a clear business need, the Security Officer may assign a generic or group user ID to more than one individual.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 36 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

b) *Password*

- 1) At a minimum, all system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on a quarterly basis.
- 2) All production system-level passwords must be part of an administered global password management database.
- 3) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- 4) User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- 5) Passwords must not be inserted into email messages or other forms of electronic communication.
- 6) All user-level and system-level passwords must be strong, minimum of six characters and containing digits, letters and symbols.

20. EMERGENCY ACCESS PROCEDURE

- a. Emergency access should be used only when normal processes to access ePHI are insufficient.
- b. If an authorized user is unable to gain access to DOC's network, information system or applications containing ePHI, the IT Help Desk should be contacted.
- c. The IT help desk will fax or email the minimum necessary ePHI after verifying the identity of the requesting authorized user.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 37 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
		SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)	
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- d. Verification shall include the name, position, callback number of the authorized user, all of which shall be tested before emergency access is granted.
- e. Emergency access shall be terminated as soon as it is no longer necessary.
- f. All activities related to emergency access shall be documented by the Security Officer or designee.

21. AUTOMATIC LOGOFF. Users of the ePHI system shall ensure that unattended personal computer stations are either logged off or that the security screen features are engaged. Users shall also terminate communication links when they are not in use in accordance with SOP 2420.2, "Information Security".

22. ACCEPTABLE ENCRYPTION

- a. Based on security risk assessment, encryption shall be used to protect all data containing ePHI stored or transmitted on certain DOC devices and hardware, such as laptops, PCs, portable digital assistants (PDAs) and removable media devices.
- b. *Data at Rest:* These items shall be protected by either encryption or firewall with strict access controls that authenticate the identity of those individuals accessing the ePHI.
- c. *Removable Media:* These items (CD-ROMs, backup tapes, and USB memory drives) shall be encrypted, if they contain ePHI.
- d. *Transmission Security:*
 - 1) All emails with ePHI transmitted outside of DOC network must be encrypted.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 38 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 2) Any ePHI transmitted through a public network (e.g., Internet) to and from vendors, clients or other third parties must be encrypted or be transmitted through an encrypted tunnel.
 - 3) ePHI must be transmitted through a tunnel encrypted (such as virtual private networks (VPN) or point-to-point tunnel protocols (PPTP) like SSL).
 - 4) ePHI shall not be transmitted through the use of web email programs.
- e. *Portable Devices:*
- 1) ePHI stored on portable devices (e.g., laptops, PDAs, etc.) must be encrypted.
 - 2) Portable devices shall not be used for the long-term storage of any ePHI.
 - 3) Portable devices that store or transmit ePHI must have installed in them proper protection mechanisms, such as antivirus software, firewall software, etc.

23. AUDIT CONTROLS

- a. Audit controls shall be set up to ensure that system users are accountable for their actions and to ensure deterrence to improper actions. To this end, the Security Officer shall ensure the following:
- b. Appropriate DOC workforce in charge of systems, applications, and devices that receive, store, transmit, or otherwise access ePHI are educated about the audit control features and functionality of their systems.
- c. Appropriate audit control features are turned “on” and utilized in all systems, applications, and devices that receive, store, transmit, or otherwise access ePHI.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 39 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- d. The need to upgrade systems, applications or devices that receive, store, transmit or otherwise access ePHI that do not have adequate audit control features and functionality.
- e. Audit control features and functionality are considered in purchase decisions for systems, applications, and devices that receive store, transmit, or otherwise access ePHI.
- f. Adequate systems storage is available for the storage of audit control information.
- g. On a yearly basis, relevant systems/applications are inventoried and assessed, and infrastructure is reviewed and tested.
- h. The Security Officer shall also determine:
 - 1) What information should be captured by audit control features and functionality within each system, application and device.
 - 2) Which audit control reports must be generated from each system, application and device.
 - 3) How often audit control reports should be generated and in what manner.
 - 4) Who will receive and review the audit control information.
 - 5) Procedures for documenting and reporting audit control discrepancies.
 - 6) The length of time and the manner in which DOC shall store the generate audit control information.

24. DATA INTEGRITY

- a. The Security Officer shall ensure there is data integrity control against the risk of:

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 40 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- 1) Unintentional modification or deletion by authorized or unauthorized user or program, and
- 2) Intentional modification or deletion by an authorized or unauthorized user.

25. PERSON OR ENTITY AUTHENTICATION

- a. Only properly authenticated and authorized persons or entities shall access ePHI maintained by the DOC.
- b. At a minimum, authentication shall require a unique user identification (“user ID”) and password combination.
- c. The Security Officer shall perform periodic validation that no redundant authentication credentials have been issued or are in use.
- d. Upon separation from DOC, a user’s account shall be cancelled or disabled.

26. CORRECTIONAL INSTITUTIONS AND OTHER LAW ENFORCEMENT CUSTODIAL SITUATIONS

For the purposes of the following disclosures in subsection a-g below, an individual is no longer an inmate when released on release, parole, probation, supervised release, or otherwise is no longer in lawful custody.

A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the protected health information is necessary for:

- a. The provision of health care to such individuals;
- b. The health and safety of such individual or other inmates;
- c. The health and safety of the officers or employees of or others at the correctional institution;

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 41 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- d. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
- e. Law enforcement on the premises of the correctional institution; or
- f. The administration and maintenance of the safety, security, and good order of the correctional institution.
- g. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

27. DISCLOSURE OF PROTECTED HEALTH INFORMATION TO LAW ENFORCEMENT OFFICIALS

Disclosures of PHI for law enforcement purposes are permitted as set forth below.. Except when required by law, the disclosures to law enforcement summarized are subject to a minimum necessary determination by the covered entity. When reasonable to do so, DOC as the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose. Moreover, if the law enforcement official making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information.

- a. To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer (signed by a judge), or a grand jury subpoena (signed by a judge). HIPAA recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information.
- b. To respond to an administrative request, such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 42 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- c. To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures of PHI to name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request.
- d. To respond to a request for PHI about a victim of a crime, and the victim agrees and executes a HIPAA compliant release. If, because of an emergency or the person's incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested.
- e. Child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required.
- f. Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such reports:
- g. If the individual agrees and the covered entity is provided a HIPAA compliant release executed by the individual;
- h. If the report is required by law; or If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations.
- i. Notice to the individual of the report may be required per HIPAA.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 43 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

- j. To report PHI to law enforcement when required by law to do so such as gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.
- k. To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.
- l. Information about a decedent may also be shared with medical examiner to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties.
- m. To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity's premises..
- n. When responding to a medical emergency, as necessary to alert law enforcement about criminal activity, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime.
- o. When consistent with applicable law and ethical standards:
- p. To a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public. Such as to identify or apprehend an individual who appears to have escaped from lawful custody.
- q. For certain other specialized governmental law enforcement purposes, such as to federal officials authorized to conduct intelligence, counter-intelligence, and other national security activities under the National Security Act or to provide protective services to the President and others and conduct related investigations.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	January 18, 2018	Page 44 of 43
PROGRAM MANUAL		SUPERSEDES:	1300.3 December 15, 2003	
		REVIEW DATE:	January 18, 2019	
SUBJECT:	HEALTH INFORMATION PRIVACY (HIPAA)			
NUMBER:	1300.3A			
Attachments:	Attachments 1 –2			

28. LITIGATION DISCOVERY DISCLOSURE

A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

- a. In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or
- b. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if :
 - 1) The covered entity receives a satisfactory HIPAA compliant release executed by the individual whose PHI is sought release provided that the covered entity discloses only the protected health information expressly authorized by such release; or
 - 2) The covered entity receives satisfactory assurance that the parties to the dispute giving rise to the request for information have agreed to a qualified protective order issued by the court or administrative tribunal with jurisdiction over the dispute that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

DOC/PM 1300.3A/1/18/2018

**D.C. Department of Corrections
Designated Record Sets**

Covered Component

Data	Data Content	Data Owner/Contact	Location	IIHI	Media (P or E)¹	Used to Make Decisions	Client Access	Comments

¹ "P" for paper medium; "E" for electronic medium.

**GOVERNMENT OF THE DISTRICT OF COLUMBIA
DEPARTMENT OF CORRECTIONS**

Access to Application

*(Use this form to **approve, deny** or **remove** an employee's right of access to application. The form shall be filled out and submitted to OMITS, ADP offices, 1901 D Street, SE. OMITS staff shall notify the employee of action taken. For assistance in completing the form, please contact DOC OMITS Help Desk at 202-523-7100.)*

Employee Name: _____ Position Title: _____
Location: _____ Telephone No.: _____
Employee is a Supervisor: Yes ___ No ___ Post Assignment: _____
Status: New ___ Reassigned ___ Previous Post _____

Application Affected

JACCS Lotus Notes Justis
 Logician Courtview Other (Specify)
 E-mail Wales Other (Specify)
 Crystal Reports Prism Other (Specify)

Logician Rights:

Group _____ Role _____ Specialty _____

Right of Access

Approved Denied Removed

Supervisor Signature: _____ Date: _____