Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 5400.01
December 30, 2022

Director, J-1

SUBJECT: Privacy and Civil Liberties Compliance

References: See Enclosure 1.

1. PURPOSE. This Defense Health Agency-Administrative Instruction (DHA-AI) based on the authority of References (a) and (b), and in accordance with the guidance of References (c) through (aq), establishes the Defense Health Agency's (DHA) procedures for achieving and managing compliance within the DHA for the following functions: Health Insurance Portability and Accountability Act (HIPAA) policy development and guidance, privacy and civil liberties regulatory compliance program and initiatives, privacy risk management within the risk management framework (RMF), privacy and civil liberties training and education, breach prevention and response, and Civil Liberties functions for the military medical treatment facilities (MTF)/dental treatment facilities (DTF). Implementation of the Religious Freedoms under the civil liberties program is not incorporated into this publication and will follow in a supplemental policy.

2. APPLICABILITY. This publication applies to the DHA personnel: assigned, attached, allotted, or detailed to the Direct Reporting Markets (Markets), the Small Market and Stand-Alone MTF Organizations (SSO), Defense Health Agency Region Europe, Defense Health Agency Region Indo-Pacific, and MTFs/DTFs.

3. POLICY IMPLEMENTATION. It is the DHA's instruction, pursuant to References (e) through (g), that:

a. The DHA Privacy and Civil Liberties Office (PCLO) will administer, manage, and provide oversight of Privacy/HIPAA programs within the Markets/SSO/DHARs/MTF/DTF. This includes HIPAA policy development and guidance, regulatory compliance and initiatives, training and education, complaints processing, breach prevention and response, and Civil Liberties functions.

b. Failure to observe the prohibitions and mandatory provisions as stated throughout this DHA-AI by military personnel is a violation of Reference (d), Article 92(1), "Failure to Obey Order or Regulation". Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to applicable laws and the terms of the contract. The terms "must", and "will" denote mandatory actions in this instruction.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. PROPONENT AND WAIVERS. The proponent of this publication is the Director, DHA Administration & Management (J-1). When Activities are unable to comply with this publication the activity may request a waiver that must include a justification and an analysis of the risk associated with not granting the waiver. The activity director or senior leader will submit the waiver request through their supervisory chain to the Director, J-1 to determine if the waiver may be granted by the Director, DHA or their designee.

7. RELEASABILITY. **Cleared for public release**. This publication is available on the Internet from the Health.mil site at: https://health.mil/Reference-Center/Policies and also available to authorized users from the DHA SharePoint site at: https://info.health.mil/cos/admin/pubs/SitePages/Home/aspx. Additional questions regarding this publication can be sent to the DHA PCLO at: dha.ncr.admin-mgt.mbx.dha-privacyguidance@health.mil.

8. EFFECTIVE DATE. This publication:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date, in accordance with Reference (c).

9. FORMS. The following DD forms can be found at: https://www.esd.whs.mil/Directives/forms

a. DD Form 2930, Privacy Impact Assessment (PIA)

b. DD Form 2959, Breach of Personally Identifiable Information (PII) Report

PLACE.RONALD.JOSEPH.1146823900

Digitally signed by PLACE.RONALD.JOSEPH.1146823900
Date: 2022.12.30 15:04:24 -05'00'

RONALD J. PLACE
LTG, MC, USA
Director

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES....5

ENCLOSURE 2: RESPONSIBILITIES....7
DIRECTOR, DEFENSE HEALTH AGENCY....7
CHIEF, DEFENSE HEALTH AGENCY PRIVACY AND CIVIL LIBERTIES OFFICE....7
DIRECTORS, MARKET, SSO, DHARs....8
PRIVACY LIAISON, MARKET, SSO, DHARs....8
DIRECTORS, MILITARY MEDICAL TREATMENT FACILITY/DENTAL TREATMENT FACILITY....9
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY OFFICER MILITARY MEDICAL TREATMENT FACILITY/DENTAL TREATMENT FACILITY....10
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SECURITY OFFICER MILITARY MEDICAL TREATMENT FACILITY/DENTAL TREATMENT FACILITY....11

ENCLOSURE 3: PROCEDURES....13
FEDERAL PRIVACY COMPLIANCE....13
DATA SHARING AGREEMENTS COMPLIANCE....15
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT POLICY....17
PRIVACY REVIEWS WITHIN RISK MANAGEMENT FRAMEWORK....17
BREACH RESPONSE AND PREVENTION....18
COMPLAINTS....19
PRIVACY TRAINING....22
CIVIL LIBERTIES COMPLIANCE....23
PRIVACY COMPLIANCE REVIEWS....23
COMPLIANCE REPORTING....24

GLOSSARY....25
PART I: ABBREVIATIONS AND ACRONYMS....25
PART II: DEFINITIONS....26

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013, as amended
(c) DHA-Procedural Instruction 5025.01, "Publication System," April 1, 2022
(d) 10 U.S.C § 892 Article 92(1); Failure to obey order or regulation
(e) 10 U.S.C. §1073c: Administration of Defense Health Agency and Military Treatment Facilities
(f) OSD Records Disposition Schedules, current edition.
(g) DoD Instruction 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs," March 13, 2019
(h) DoD Manual 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Healthcare Programs," March 13, 2019
(i) DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015
(j) DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology (IT)," July 19, 2022
(k) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(l) 5 U.S.C, Section 552a - "Records maintained on individuals" as part of Privacy Act of 1974, as amended.
(m) Public Law 107-347, "E-Government Act of 2002," December 17, 2002
(n) DHA- Administrative Instruction 75, "Health Insurance Portability and Accountability Act (HIPAA) Core Tenets Procedures," December 2, 2014,
(o) DHA- Administrative Instruction 74, "Workforce Training Pursuant to the Requirements of the Privacy Act and Health Insurance Portability and Accountability Act," December 2, 2014
(p) DHA-Administrative Instruction 71, "Incident Response Team (IRT) and Breach Response Requirements," September 15, 2015
(q) Public Law 111-5, Title XIII, Subtitle D, "Health Information Technology for Economic and Clinical Health (HITECH) Act," February 17, 2009
(r) ASD(HA) Memorandum for the Services, "Request to Appoint Military Treatment Facility/Dental Treatment Facility Health Insurance Portability and Accountability Act Privacy Officer," June 18, 2002[1]
(s) ASD(HA) Memorandum for the Services, "Request to Appoint Medical Treatment Facility and Dental Treatment Facility [HIPAA] Security Officials," September 9, 2004
(t) Public Law 113-283, "Federal Information Security Modernization Act of 2014," December 18, 2014

[1] This reference can be found at: https://www.health.mil/Reference-Center/Policies/2002/06/18/DHA-HIPAA-Privacy-Officers-Appointment-Request-Letter

(u) DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended
(v) National Institute of Standards and Technology Special Publication 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010
(w) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended
(x) Office of Management and Budget Circular No. A-130, "Managing Information as a Strategic Resource," July 28, 2016
(y) Office of Management and Budget Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," December 23, 2016, as amended
(z) DoD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use within DoD," August 1, 2012, as amended
(aa) DHA Procedural Instruction 8160.01, "Defense Health Program (DHP) System Inventory Management and Reporting," May 13, 2019
(ab) DHA Procedural Instruction 8140.01, "Acceptable Use of Defense Health Agency Information Technology (IT)," October 16, 2018
(ac) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended
(ad) DoD Directive 5100.01, "Functions of the Department of Defense and Its Major Components," December 21, 2010, as amended
(ae) DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021
(af) Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017
(ag) Code of Federal Regulation, Title 45, Part 160 and 164
(ah) DoD Instruction 3216.02, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research," April 15, 2020, as amended
(ai) National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020, as amended
(aj) DHA-Administrative Instruction 5015.01, "Records Management," February 6, 2020
(ak) DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections" June 30, 2014, as amended
(al) Code of Federal Regulation, Title 32, Part 2002, "Controlled Unclassified Information"
(am) DoD Instruction 1100.13, "Department of Defense Surveys," March 31, 2017, as amended
(an) DHA-Administrative Instruction 101, Processing Procedures for Complaints Involving Discrimination in Military Health System (MHS) Health Programs and Activities, September 14, 2018.
(ao) DHA-Administrative Instruction 064, "Civil Liberties Program," June 14, 2017
(ap) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," August 11, 2017.

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, will maintain overall responsibility for the implementation of this publication to safeguard the privacy and security of personally identifiable information (PII)/protected health information (PHI) entrusted to the DHA and to ensure reasonable and adequate safeguards are maintained for all such PII/PHI created, maintained, received, or transmitted through electronic or non-electronic media.

2. CHIEF, DHA PRIVACY, AND CIVIL LIBERTIES OFFICE. To ensure compliance with all applicable statutory, regulatory, and policy requirements to manage privacy safeguards and risks, the Chief, DHA PCLO, will:

a. Develop and administer policies and procedures governing the collection, maintenance, use, and disclosure of PII and PHI for the DHA. In addition, the Chief, DHA PCLO, will provide guidance to help ensure the safeguarding of PII/PHI across the Military Health System in a separate issuance.

b. If or when acting as the designee of the Senior Component Office for Privacy (SCOP), will review authorization packages for those MTF/DTF information systems (IS) that, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII/PHI to ensure compliance with applicable privacy requirements and manage privacy risks; and coordinate with authorizing officials on granting authority to operate (often referred to as "ATO") decisions for IS. The Chief, DHA PCLO, when acting on behalf of and as designee of the SCOP, will review all authorization packages for systems that process PII and/or PHI.

c. Execute a Data Sharing Compliance Program for DHA managed data to ensure compliance with HIPAA and Reference (l).

d. Serve as the central DHA point of contact (POC) for receiving all DHA breach reports; provide direction and oversight to the Action Officer (AO) to ensure compliance with all requirements, including reporting, individual notification, internal and external communications, and necessary mitigation steps of all MTF/DTF breaches.

e. Facilitate the resolution of reported Privacy Act, Civil Liberties, and HIPAA violations and complaints pertaining to the DHA to include initiating investigations, adjudicating findings, and fulfilling necessary reporting requirements.

f. Establish, conduct, and monitor Privacy Act, HIPAA, and Civil Liberties training requirements for the DHA.

g. Establish the methodology to conduct and monitor annual HIPAA Privacy and Security Compliance Risk Assessments.

h. Establish requirements to conduct an annual HIPAA Privacy and Security Compliance Risk Assessment for the direct reporting Markets, the SSO, the DHARs, the MTFs, and the DTFs. .

i. Develop requisite compliance reports and coordinate input from the direct reporting Markets, the SSO, the DHARs, the MTFs, and the DTFs as necessary.

j. Provide oversight for the DHA Privacy Boards for research.

3. DIRECTORS, Markets, SSO, DHARs. The Directors will:

a. Notify MTFs/DTFs Directors of their requirement to identify and designate the MTF/DTF HIPAA Privacy Officer (HPO) and HIPAA Security Officer (HSO). A DoD covered entity's HPO may also be dual hatted as the designated HSO for that DoD covered entity, as provided in Reference (i).

b. Coordinate and verify that the DHA PCLO is notified of MTF/DTF HPO/HSO appointments for each of its reporting facilities to ensure DHA PCLO maintains a current POC roster of HPO/HSOs.

c. Ensure the appointment or fulfillment of the Markets, SSO, DHARs, Privacy Liaison position.

d. Ensure their Markets, SSO, DHARs Privacy Liaisons receive the education and training that DHA PCLO provides through their monthly education and training opportunities (PMET), quarterly Health Information Privacy & Security Compliance Committee meetings (HIPSCC), the annual Health Information Privacy and Security (HIPS) training, and any other DHA PCLO directed scheduled trainings, relevant to the Privacy Liaison duties and responsibilities. *NOTE: In the event a* Markets, SSO, DHARs *Privacy Liaison is unable to attend the scheduled training, due to authorized leave, the Privacy Liaison will contact training: dha.ncr.pcl.mbx.privacy-training@health.mil for the recorded link of the training session.*

4. PRIVACY LIAISON, Markets, SSO, DHARs. The DHA PCLO will fulfill the responsibilities outlined in this section until Privacy Liaison positions are established within the respective Markets, SSO, DHARs. Once established, the Markets, the SSO, the DHARs, Privacy Liaison will:

a. Act as an intermediary between MTFs/DTFs and the DHA PCLO, to include performing all related responsibilities outlined in the procedures found in Enclosure 3 of this DHA-AI.

b. Coordinate with the DHA PCLO on the management of Privacy Impact Assessments (PIA) and Data Sharing Agreements (DSA).

c. Work with MTF/DTF HPOs/HSOs to manage privacy related risk and requests for information (RFI).

d. Disseminate and ensure compliance with DHA PCLO policy and guidance. The Markets, SSO, DHARs Privacy Liaison will also support MTFs/DTFs adherence to DoD and other Federal Regulations.

e. Coordinate with MTF HSOs/HPOs to manage HIPAA investigations, while the DHA PCLO will oversee the complaints process and support investigations when needed. The DHA PCLO will act as the liaison to the Department of Health and Human Services (HHS)/Office for Civil Rights (OCR).

f. Coordinate with MTF HPOs/HSOs to resolve HIPAA policy and guidance inquiries. The Markets, SSO, DHARs Privacy Liaison will escalate complex policy and guidance queries to the DHA PCLO.

g. Coordinate with the DHA PCLO on privacy risk management within RMF.

h. Coordinate with MTF HPOs/HSOs to oversee breach investigations and ensure proper mitigations have been implemented.

i. Attend and complete training maintain responsibility in accordance with DHA PCLO requirements.

j. The Markets, SSO, DHARs will maintain compliance with DHA PCLO issuances.

k. Track training compliance for their MTF/DTF HPOs/HSOs and submit- compliance trackers to DHA PCLO when requested.

l. Coordinate with the DHA PCLO to lead HIPAA Privacy and Security Compliance Risk Assessment.

m. Ensure MTF/DTF HPO/HSO receive the education and training that the PCLO provides through the DHA PMET, Quarterly HIPSCC, Annual HIPS, and any other DHA PCLO directed scheduled trainings, relevant to the HPO/HSO/Privacy Liaison duties and responsibilities.

5. DIRECTORS, MTF/DTF. The MTF/DTF Directors will:

a. Ensure facility policy and procedures remain current and conform to this publication.

b. Review the organizational structure and align the Privacy and HIPAA Privacy/Security staff based on size of the facility, location, staff skills.

c. Identify and designate MTF/DTF HPO/HSO, in accordance with References (s) and (t), who will have the overall responsibility for maintaining the privacy and protection of health information; ensure compliance with federal laws and regulations; and develop appropriate organizational initiatives. A DoD covered entity's HPO may also be the designated HSO for that DoD covered entity as provided in Reference (i).

d. Notify DHA PCLO and Markets, SSO, DHARs of the appointments or designation of MTF/DTF HPO/HSO via official memorandum upon designation; notify the DHA PCLO of any changes to the appointment within two weeks of appointment and within two weeks of any change in personnel. A staff member may be designated to multiple roles at the MTF/DTF Director's discretion.

e. Ensure appropriate personnel actions are taken for non-compliance with handling of PII/PHI.

f. Identify and coordinate with a Markets, SSO, DHARs Privacy Liaison, as needed, to ensure privacy matters are addressed appropriately.

g. Ensure all HPO/HSO receive the education and training that the PCLO provides through the DHA PMET, Quarterly HIPSCC, Annual HIPS, and any other DHA PCLO directed scheduled trainings, relevant to the HPO/HSO duties and responsibilities.

6. HIPAA Privacy Officer, MTF/DTF. In addition to the responsibilities outlined in Reference (h), the MTF/DTF HPO will:

a. Ensure any external requests to use data managed by the DHA at the local MTF/DTF level are routed to the DHA PCLO for review and approval.

b. Serve as the designated AO for the organization with overall responsibility for coordinating information flow and response actions to breaches of PII or PHI.

c. Ensure disclosures of PII/PHI are documented in either the Protected Health Information Management Tool (commonly referred to as "PHIMT"), the HIPAA disclosure accounting mechanisms on the MHS GENESIS platform, or any other DHA PCLO approved accounting tool.

d. Serve as the central POC to receive HIPAA and Privacy Act complaints for investigation and resolution.

e. Ensure organizational leadership is included in all correspondence pertaining to breach-related events and response activities through updates and other reporting requirements as applicable.

f. In coordination with the HPO/HSO's respective Market, SSO or DHAR Privacy Liaison report a confirmed cybersecurity incident, contact DHA Cyber Operations Center within one

hour at: dha.jbcharleston.j-6.list.cyber-operations-center@health.mil. All confirmed cyber-related breaches involving PII and PHI must be reported to the DHA Cyber Operations Center within one hour of being confirmed.

g. In coordination with the HPO/HSO's respective Market, SSO or DHAR Privacy Liaison, report all breaches to the DHA PCLO within 24 hours of discovery, using DD Form 2959, Breach of Personally Identifiable Information (PII) Report via e-mail to: dha.ncr.pcl.mbx.dha-privacy-officer@health.mil.

h. In coordination with the HPO/HSO's respective Market, SSO or DHAR Privacy Liaison, conduct administrative investigations into breaches and provide the investigative findings and responses to the DHA PCLO for final breach risk analysis determination in accordance with Reference (p).

i. Maintain records consisting of HIPAA and Privacy Act remedial training, counseling documents, and administrative actions or sanctions imposed on workforce members for confirmed violations as required by HIPAA and other federal requirements in accordance with Reference (aj).

j. Ensure the MHS Notice of Privacy Practices is available and provided to beneficiaries.

k. Coordinate with Markets, SSO, DHARs Privacy Liaison to:

(1) Complete all necessary trainings to include HPO/HSO Training within Joint Knowledge Online (JKO).

(2) Submit and/or escalate RFI and receive guidance on policy.

(3) Inform Markets, SSO, DHARs Privacy Liaison of significant risks or impacts to MTF/DTF Privacy Operations.

(4) Complete tasks as outline in Enclosure 3 of this DHA AI.

l. Attend all DHA PMET, Quarterly HIPSCC, Annual HIPS, and any other DHA PCLO directed scheduled trainings, relevant to the HPO/HSO duties and responsibilities. *NOTE: In the event an HPO/HSO is unable to attend the scheduled training, due to an authorized leave of absence the HPO/HSO will contact training for the recorded link of the training session.*

7. HSO, MTF/DTF. In addition to those specific responsibilities outlined in References (g) and (i), the MTF/DTF HSO will:

a. Coordinate with the HPO, DHA PCLO, and Risk Management Executive Division (RMED) on security incidents impacting electronic PHI (ePHI).

b. Evaluate and develop local HIPAA Security compliance procedures in coordination with the DHA PCLO.

c. Assess and respond to local HIPAA Security inquiries in accordance with policies developed by the DHA PCLO.

d. Conduct annual HIPAA Privacy and Security Compliance Risk Assessment based on policies developed by the DHA PCLO and provide findings and report to the DHA PCLO.

e. Coordinate with Markets, SSO, DHARs Privacy Liaison to:

(1) Complete all necessary trainings to include HPO/HSO Training within JKO.

(2) Submit and/or escalate RFI and receive guidance on policy.

(3) Inform Markets, SSO, DHARs Privacy Liaison of significant risks or impacts to MTF/DTF Privacy Operations.

(4) Complete tasks as outline in Enclosure 3 of this DHA-AI.

ENCLOSURE 3

PROCEDURES

1. FEDERAL PRIVACY COMPLIANCE. Pursuant to References (m) and (n), DHA must comply with federal privacy legislation and associated DoD regulations and instructions, Office of Management and Budget, and National Institute of Standards and Technology guidance. As such, DoD and DHA have published official policies and procedures implementing the requirements of the Reference (k) and Reference (u).

a. System of Records Notices (SORN). The DHA must publish a notice in the Federal Register for systems of records (SOR) where records are retrieved, in accordance with Reference (l), by an individual's name or other PII that uniquely identifies or links to an individual.

(1) Requests to publish a new SORN or modify, amend, or rescind an existing SORN for any DHA SOR must be submitted by IT managers/owners to DHA PCLO for review via e-mail to: dha.ncr.pcl.mbx.privacyactmail@health.mil. The DHA PCLO will coordinate with the DHA Information Management Control Office (IMCO) to submit the request to Defense Privacy, Civil Liberties, and Freedom of Information Act Directorate (DPCLFD) for approval and publication in the Federal Register.

(2) Any request to claim a Privacy Act Exemption for a SOR must be reviewed by the DHA Office of General Counsel prior to submission to the DHA PCLO for review and further coordination.

(3) Compliance with Reference (an) is under the purview of the IMCO. The DHA PCLO will facilitate compliance reviews with the DHA IMCO for SORs and SORNs.

(4) DHA Components and MTFs/DTFs are required to ensure SORNs submitted to DHA PCLO for review and submission to DPCLFD are compliant with Reference (l) by working with their respective records manager.

b. Social Security Number (SSN) Justification Memorandums. The collection, use, or retention of the SSN in any form, system, application, shared drive, web portal, or other repository (e.g., full, truncated, masked, partially masked, encrypted, or disguised SSNs) pursuant to the DoD acceptable use criteria must be documented in an SSN Justification Memorandum and approved by DPCLFD.

(1) Memoranda must be submitted to the DHA PCLO for review via e-mail to: dha.ncr.pcl.mbx.privacyactmail@health.mil. The DHA PCLO will work with the AO to ensure the justification package is complete and ensure there is a plan to eliminate the SSN (if possible), prior to submission to DPCLFD for approval and signature.

(2) Memoranda are effective until and unless there are significant changes to the associated IS, form, or other information collection that would make the information contained

in the original memorandum outdated or inaccurate. In such instances, stakeholders should consult with the DHA PCLO to determine whether a new memorandum is required. The DHA PCLO will additionally consult with DPCLFD on these matters.

c. Information Collections. Requests to implement a new DHA information collection (i.e., forms and surveys) or modify an existing collection must be routed through the DHA Forms Management Officer and DHA IMCO as appropriate, in accordance with Reference (am).

d. Privacy Act Statement & Advisories. A Privacy Act Statement must be provided when PII is collected directly from an individual, placed into a SOR, and retrieved by a personal identifier. The statement provides the individual with information necessary to make an informed decision about whether to provide that information. A Privacy Advisory is required whenever accessing a system which may contain PII.

(1) The DHA PCLO will advise on the requirement for a Privacy Act Statement or Advisory.

(2) Privacy Act Statements and privacy advisories must be submitted to the DHA PCLO for review via e-mail to: dha.ncr.pcl.mbx.privacyactmail@health.mil.

e. Privacy Impact Assessment. A PIA must be performed on DoD IT and electronic collections, including those supported through contracts with external sources, that collect, maintain, or disseminate PII. PIAs must be updated by system owner/manager in accordance with Reference (x) and (ap).

(1) Use of the DD Form 2930, Privacy Impact Assessment is mandatory for all PIA submissions. The DD Form 2930 should be coordinated with DHA J-6, RMED, and the DHA PCLO in accordance with References (x) and (ap).

(2) Once signed by the DHA CIO, J-6, the PIA is considered fully executed and will remain valid for a period of 3 years, generally. For additional details, see Paragraph 5 of this enclosure, and within Reference (u). If a system or collection with a completed PIA is significantly changed and creates new privacy risks, the privacy risk posture must be reassessed with a new PIA. *NOTE: The term "significantly changed" is an intentionally broad, catchall term. Some examples include significant system management changes, significant merging, new interagency uses, alteration in character of data (e.g., when new PII is added to a collection), or if there are changes in a systems actual retrieval of records subject to the Privacy Act*.

(3) Once the fully executed PIA is received, a Section 508 compliant version of Section 1 of the PIA will be posted for the public on health.mil in accordance with Reference (ap).

(4) A copy of the fully executed PIA will be provided to the OSD, Office of the DoD CIO.

(5) For PIAs at the MTF/DTF level, Markets, SSO, DHARs will review and coordinate the Program Manager/Designee and Information System Security Manager signatures for those

PIAs. Once signed, PIAs should be sent to DHA for review and coordination in accordance with References (x) and (ap).

2. DATA SHARING AGREEMENTS COMPLIANCE. Pursuant to References (h) and (l), DHA must ensure certain privacy and security protections are met before sharing PII or PHI and specific privacy language is included in DSAs depending on the data shared and the purpose for which it is shared. In addition, References (w), (y), (z), (x), (ah), and (ai) outline best privacy practices and provides specific security and privacy controls that must be met in sharing data through contracts. The DHA PCLO receives various types of research and non-research requests for DHA data. Under the DHA's Data Sharing Program, the DHA PCLO uses DSAs as administrative controls to review each requested use of DHA data for compliance with applicable federal law and implementing DoD policies.

a. Criteria for a DSA:

(1) Requested by outside parties such as contractors, universities, academic researchers, researchers supported in a DoD-supported study, or other non-government personnel.

(2) For government personnel conducting research. *Note: For government only research a Data Sharing Agreement Application (DSAA) is not required when the data being requested is for de-identified data or when the data contains PHI where appropriate authorizations have been obtained for entities under the auspice of the DHA*.

b. Before requesting a DSA, all non-research requestors must submit a Prerequisite Checklist to ensure that they obtain the necessary documentation and approval is obtained before a packet is submitted. The Prerequisite Checklist must be requested at: dha.ncr.j-6.mbx.dsa-mail@health.mil. The checklist is a mechanism used to prescreen the request to determine if a DSA is needed.

(1) If a DSA is needed, the requestor must submit a DSAA and supporting documents to the DHA PCLO for review and approval at: dha.ncr.j-6.mbx.dsa-mail@health.mil. If the requestor is based at an MTF/DTF, the requestor will first send their DSAA to their respective Markets, SSO, DHARs Privacy Liaison for initial review. The Markets, SSO, DHARs Privacy Liaison will work with the MTF/DTF requestor on any necessary changes to the DSAA. The Markets, SSO, DHARs Privacy Liaison will then coordinate with DHA PCLO for processing.

(2) If a DSA is not needed, the DHA PCLO will issue a "No Action Letter" to the requestor.

c. The DHA PCLO will incorporate the approved DSAA into the final executed DSA.

d. If necessary, the DHA PCLO Security Team will review HIPAA Safeguard Review of Non-Federal Systems Templates for systems that do not have a required DoD authorization decision to determine if the privacy and security posture of an organization is conclusive in nature or may be vulnerable to cyber intrusive breach.

e. For research requests that include the use of DHA Protected Health Information, the DHA PCLO will verify there is adequate documentation of HIPAA Privacy Rule reviews (e.g., Institutional Review Board (IRB) approvals of a research a protocol's HIPAA authorization template or HIPAA waivers of authorization) for HIPAA Privacy Rule compliance. When sharing a Limited Data Set, DHA's PCLO will verify that appropriate HIPAA Privacy Rule documentation have been met. Research pursuant to a contract must adhere to requisite data requirements of Reference (al).

f. The DHA PCLO will send a PDF version of the executed DSA, with approved DSAA to the applicant, government sponsor, and DHA Agreements Manager for their records.

g. For research studies or activities requesting DHA data, applicants must comply with the requirements in Reference (ak) before submitting a DSAA. Applicants must provide evidence the project has received appropriate review and approval or exemption (e.g., documentation of the IRB or EDO approval letter).

h. The DHA PCLO is responsible for auditing and oversight of all DHA Privacy Boards under the IRB's Streamlining Program which ensures the HIPAA Privacy Rule compliance is adhered to for research utilizing DHA protected health information.

(1) The DHA Privacy Boards will ensure the DHA HIPAA Privacy Rule templates are used to ensure compliance with DHA policies and procedures.

(2) DHA Privacy Boards will assist researchers and the research community by responding to inquiries related to HIPAA compliance requirements. All inquiries that are not answered by the DOD IRB/Privacy Review Board may be submitted to the DHA PCLO via e-mail to: dha.ncr.pcl.mbx.privacyboard@health.mil.

(3) The DHA Privacy Boards will collaborate and educate the DHA research community on HIPAA Privacy Rule compliance requirements through the IRBs Streamlining Program. The program provides a uniform method for HIPAA Privacy Rule data determinations. It also documents the method and determination for compliance with HIPAA recordkeeping requirements.

(a) An IRB that will participate in the IRBs Streamlining Program must fulfill all requirements outlined by the DHA PCLO.

(b) DHA PCLO will provide a Letter of Completion to IRBs once they complete the requirements to participate in the Research Streamlining Initiative.

(c) DHA PCLO delegates all data determinations and HIPAA Privacy Rule reviews to DHA Privacy Boards and/or DoD IRBs who will ensure understanding and compliance with the HIPAA Privacy Rule requirements.

(d) IRBs participating in the IRB Streamlining Initiative may submit requests for guidance via e-mail to: dha.ncr.pcl.mbx.privacyboard@health.mil.

3. HIPAA POLICY. DHA PCLO must implement and maintain reasonable and appropriate policies and procedures that provide privacy and security protections for all PHI maintained by DHA Components and are also consistent with the HIPAA Rules in References (g), (h), (n), (r), (s), and in accordance with Reference (o). While MTF/DTF operations will be guided by overarching policies and procedural guidance issued by the DoD, the MTFs/DTFs must also have in place local policies and procedures addressing the implementation of such policy, which may be subject to review by the DHA PCLO. Markets, SSO, DHARs will receive and disseminate policy provided by the DHA PCLO and ensure the proper compliance at the MTF/DTF level.

a. The DHA PCLO will ensure policies and other publications are created in compliance with DoD requirements and coordinate with applicable DHA components.

b. The MTF/DTF HPO/HSO may forward any local draft MTF/DTF HIPAA Privacy and HIPAA Security policies/procedures to the DHA PCLO for review upon request.

c. Inquiries or policy specific guidance regarding implementation of the HIPAA Rules and regulations within the MHS will be addressed by the local HPO/HSO or may be routed to their Markets, SSO, DHARs Privacy liaisons or DHA PCLO for guidance, as appropriate. Inquiries may be submitted via e-mail to: dha.ncr.admin-mgt.mbx.dha-privacyguidance@health.mil.

4. PRIVACY REVIEWS WITHIN RISK MANAGEMENT FRAMEWORK. Pursuant to References (i), (j), (x), (y), (ad), and (aj) a risk-based authorization decision for DoD IS and platform IT systems must be made prior to deployment within the DoD environment. For the DHA, authorization is obtained using the DHA RMF process that has been defined by the DHA Assessment and Authorization Branch of the DHA Health Information Technology (IT) RMED. The DHA RMF process defines a series of controls (i.e., requirements) that systems must have in place to address potential threats faced by the system and promotes ongoing risk management with emphasis on timely correction of deficiencies.

a. The DHA PCLO, in accordance with Reference (ai), will review all authorization packages for systems that process PII and/or PHI under the purview of the DHA CIO. DHA PCLO will coordinate with privacy counterparts to manage privacy risks throughout the RMF process when appropriate.

b. MTF/DTF HSO is responsible for maintaining an inventory of the physical systems, devices and storage media that process PII and/or PHI within their respective facility and will provide a consolidated report of MTF/DTF PII/PHI holdings to the DHA PCLO.

c. The DHA PCLO will work with the Markets, SSO, DHARs Privacy Liaisons to support Markets, SSO, DHARs through training, providing templates, verifying documents are completed, and identifying best practices.

5. BREACH RESPONSE AND PREVENTION. Enclosure 3 of References (h), (k), (q), (ae), and (af) provide the procedures for reporting, responding, and mitigating any potential or confirmed breaches of PII or PHI within the DHA.

a. All DHA workforce members will report upon discovery of a suspected or confirmed compromise of PII/PHI to their local HPO/HSO within one hour.

b. In coordination with the HPO/HSO's respective Market, SSO or DHAR Privacy Liaison, will verify with the local IT department and upon confirmation report a confirmed or suspected cybersecurity incident to DHA Cyber Operations Center within one hour at: usn.jbcharleston.niwcatlanticsc.mbx.cssp-watch@health.mil within one hour.

c. DHA Cyber Operations Center will report to U.S. Cyber Command within 48 hours as required by Reference (af).

d. Business associates who create, receive, maintain, or transmit PII/PHI will report all cybersecurity incidents that occur outside of DoD's network directly to Cybersecurity and Infrastructure Security Agency (CISA)/United States Computer Emergency Readiness Team (US-CERT) within 48 hours (e.g., Purchase Care Contractors, Vendors, Contractors, and Sub-Contractors). Additionally, Business associates will report all breaches to the DHA PCLO within 24 hours of discovery using DD Form 2959, Breach of Personally Identifiable Information (PII) Report via email: dha.ncr.pcl.mbx.dha-privacy-officer@health.mil

e. U.S. Cyber Command will report to Cybersecurity and Infrastructure Security Agency (CISA)/United States Computer Emergency Readiness Team (US-CERT) within one hour if the incident involves a confirmed cybersecurity incident (References (h) and (af)).

f. In coordination with the HPO/HSO's respective Market, SSO or DHAR Privacy Liaison, will report all breaches to the DHA PCLO within 24 hours of discovery using DD Form 2959, Breach of Personally Identifiable Information (PII) Report via email: dha.ncr.pcl.mbx.dha-privacy-officer@health.mil.

g. The DHA PCLO will report the breach using DPCLFD's breach reporting tool within 48 hours.

h. The DHA PCLO will make the determination on whether a breach notification is required on a case-by-case basis and will document a breach risk analysis for each reported breach. If notification is required, the DHA PCLO must approve the contents of the notification letter, and beneficiary notification must be made within 10 days of receiving a breach risk analysis determination.

i. The DHA PCLO will make the determination regarding whether a breach is reportable to HHS OCR.

j. The DHA PCLO will report all breaches deemed reportable to HHS OCR.

k. The HPO/HSO, and any other POCs, as designated, will provide updates to the breach reports, as appropriate to the DHA PCLO and to the identified Markets, SSO, DHARs Privacy Liaison.

6. COMPLAINTS. Pursuant to Section 7.2.a of Reference (h) and Section C10.1 of Reference (k), individuals may file complaints with DoD if they believe their privacy rights have been violated. The Privacy Act and HIPAA require organizations to make public information regarding procedures for an individual to access his or her information and to correct or amend inaccurate information. The DHA PCLO has a process to review and adjudicate privacy complaints or inquiries that arise out of MTFs/DTFs. The procedures ensure all complaints are recorded, tracked, and addressed. Complaints are submitted via e-mail to: dha.ncr.pcl.mbx.dha-privacy-office-mail@health.mil.

a. All complaints alleging violation(s) of the Privacy Act or HIPAA Rules by DHA to include the MTFs/DTFs, must be received in writing, by either the MTF/DTF or the DHA PCLO.

b. Complaints received directly to the DHA PCLO will be routed through the Markets, SSO, DHARs Privacy Liaison to the MTF/DTF HPOs/HSOs for investigation and response.

c. Investigations will be assigned to the appropriate POC, and investigations will be executed, in accordance with the instructions provided in the complaint correspondence.

(1) The MTF/DTF HPO/HSO will report any MTF/DTF-based potential breach(es) for allegations involving a potential loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for another than authorized purpose have access or potential access to PII, whether physical or electronic, in accordance with References (l), (q), and (r).

(2) The MTF/DTF HPO/HSO will submit an amended breach report to the DHA PCLO and their represented Markets, SSO, DHARs Privacy Liaison at the conclusion of the investigation confirming whether a breach occurred.

(3) The MTF/DTF HPO/HSO will ensure the individual(s) found to have violated HIPAA will be subject to, at minimum, complete HIPAA and Privacy Act remedial training and administrative actions/sanctions as deemed appropriate by the appropriate MTF/DTF leadership authority or supervisor.

(4) DHA PCLO will task DHA components via e-mail to initiate an investigation into complaints received by the DHA PCLO.

d. Investigators for alleged HIPAA violations will be assigned and investigations conducted in accordance with References (h) and (r) (as applicable) and the guidance found in this publication or succeeding publications. Investigations will, at a minimum, address all required items from the Complaints Correspondence, as applicable, and must be reviewed and endorsed by the MTF/DTF HPO/HSO.

(1) Complaints involving MTFs/DTFs, and clinics will be investigated primarily by the designated HPO/HSO.

(2) Complaints involving the other DHA Components will be investigated primarily by supervisors and local personnel responsible for compliance with Reference (s).

(3) MTF/DTF HPO/HSO will serve as the central POC to receive complaints involving their designated MTF/DTF.

(4) MTF/DTF HPO/HSO will conduct administrative investigations for complaints and respond to requests for additional information.

(5) The respective Markets, SSO, DHA Privacy Liaison will provide the investigative findings and responses to additional information requests for complaints involving MTF/DTF personnel to the DHA HIPAA Compliance Manager for review and final endorsement within 30 days of the investigation assignment. Extensions to investigations are subject to the discretion of the DHA PCLO Compliance Resolution Specialist.

(6) MTF/DTF HPO/HSO will maintain records consisting of HIPAA and Privacy Act remedial training, counseling documents, and any administrative actions/sanctions imposed for MTF/DTF personnel found to have violated HIPAA Rule in accordance with Reference (aj) and provide copies to the DHA PCLO HIPAA Compliance Manager upon request.

e. DHA PCLO HIPAA Compliance and Breach Team will forward investigation requests through the Markets, SSO, DHARs to the MTFs/DTFs for investigation. Markets, SSO, DHARs will ensure MTFs/DTFs HPOs/HSOs thoroughly investigate allegations and forward complete investigations reports to the DHA PCLO for review and determination. A copy of the endorsement memorandum closing the investigation at the DHA PCLO office will be provided for the MTF leadership, through the Privacy Liaison or HPOs/HSOs when appropriate. HPOs/HSOs should advise those seeking copies of the investigation results to submit a Freedom of Information Act (FOIA) request to the DHA FOIA Service at the following: https://www.foia.gov/. Guidance on how to submit the FOIA request for information is posted to the site.

f. Individuals responsible for investigating complaints alleging violations of the Privacy Act, and not HIPAA, arising within the DHA will be assigned based on the location of the alleged violation and the parties involved. Investigations will still address the items discussed in paragraph 5 of this enclosure.

(1) The MTF/DTF POC will be the primary investigator for complaints alleging Privacy Act violations at an MTF/DTF and where the PII involved is not protected under HIPAA. The MTF/DTF POC will review and provide determinations on all administrative investigations concerning Privacy Act violations. The MTF Director may choose to provide concurrence with these findings. The DHA PCLO will consult with supervisors, DHA Human Resources, and other stakeholders to assign an investigator for such complaints involving other locations.

(2) The assigned investigator will conduct administrative investigations for complaints and respond to requests for additional information.

(3) The assigned investigator will provide the investigative findings and responses to additional information requests for complaints involving Privacy Act violations to the DHA PCLO for review and final endorsement within 30 days of the investigation assignment. Extensions to investigations are subject to the discretion of the DHA PCLO.

(4) Documentation pertaining to remedial training, counseling, and any administrative actions/sanctions imposed for a Privacy Act violation will be maintained by supervisors with copies provided to the DHA PCLO upon request.

g. Upon receipt of a complaint to DHA PCLO alleging a Civil Liberties violation(s), arising within the DHA and its components to include MTFs/DTFs, the Markets, SSO, DHARs, and MTF/DTF POC will:

(1) Route the complaint to the DHA PCLO for proper intake, tracking, tasking, and processing.

(2) Collaborate with other resources, including but not limited to the organization's Legal and Human Resources departments to assist with complaint adjudications.

(3) Ensure the final report to the DHA PCLO includes all findings and corrective actions and are tracked accordingly for the DHA to respond and facilitate resolution.

h. Pursuant to Sections 5.4 of Reference (g) and C3.3 of Reference (k), individuals may file requests to amend their records with DoD as provided for under the Privacy Act and HIPAA; however, DoD has the right to deny such requests. Individuals have a right to appeal denials of requests to amend and DoD has the right to deny such appeals. The DHA PCLO has a process to ensure any requests to amend and appeals of denied requests to amend are appropriately routed to the appropriate DoD stakeholder. If any request to amend or appeals of a denied request to amend contain PHI, then the request or appeal will be addressed according to Section 5.4 of Reference (g) and routed to the appropriate DoD covered entity for adjudication. If any request to amend or appeals of a denied request to amend contain only PII, and no PHI, then the request or appeal will be addressed according to Section C3.3 of Reference (k) and routed to the appropriate DoD stakeholder for adjudication. For more information, e-mail the following mailbox: dha.ncr.pcl.mbx.dha-privacy-office-mail@health.mil.

7. PRIVACY TRAINING. Pursuant to References (g) and (k), HIPAA and Privacy Act training is required for all DHA civilian, military, and contractor personnel. The DHA PCLO promotes a culture of compliance through awareness, education, and outreach activities, including onboarding sessions, annual seminars, routine newsletters and publications, and in-person and virtual training events. Training inquiries or questions are submitted via e-mail to: dha.ncr.pcl.mbx.privacy-training@health.mil.

a. The DHA PCLO will determine privacy and HIPAA training requirements for DHA personnel.

b. MTF/DTFs will conduct a HIPAA and Privacy Act training overview for each staff member during newcomer orientation. Thereafter, initial, annual refresher training must be completed via JKO. Remedial training is also available where HPOs/HSOs and Training Managers can assign training out of cycle should the need arise and as determined by the user's leadership.

c. Record of completion will be maintained on the administrative section of JKO in accordance with Reference (m) and is readily available to the user and/or the Training Manager.

d. Advanced training is provided through the HPO/HSO Training on the JKO platform, for designated HPOs/HSOs, and personnel with concurrent responsibilities. This training is mandatory for all new HPOs/HSOs. The Markets, SSO, DHARs are responsible for tracking training compliance.

e. Any deviation from the standard training requirements must be approved by the DHA PCLO.

f. Additional training may be provided on specific functions performed by the PCLO at the request of MTF/DTF HPOs/HSOs.

g. MTF/DTF POCs will ensure all workforce members receive Civil Liberties training and participate in Civil Liberties training activities as directed by the DHA PCLO.

h. Markets, SSO, DHARs will support the provision/dissemination of trainings provided by the DHA PCLO, as well as provide input to the DHA PCLO on trainings needs of MTFs/DTFs.

i. In order to meet the HIPAA training requirements outlined in Reference (h) Section 7b, all Markets, SSO, DHARs Privacy Liaisons and MTF/DTF HPOs/HSOs must attend all DHA PMET, Quarterly HIPSCC, Annual HIPS, and any other DHA PCLO directed scheduled trainings, relevant to the HPO/HSO/Privacy liaison duties and responsibilities. *NOTE: In the event any are unable to attend the scheduled training due to an authorized leave of absence the Liaison or HPO/HSO will contact training: dha.ncr.pcl.mbx.privacy-training@health.mil for the recorded link of the training session.*

8. CIVIL LIBERTIES COMPLIANCE. Pursuant to References (u), (ae), and (ao), appropriate MTF/DTF POC(s) will coordinate with the DHA Civil Liberties Officer regarding inquiries arising within the DHA and its Components.

a. Reporting Requirements. Upon receipt of a RFI by the DHA PCLO related to Civil Liberties violation(s), the Markets, SSO, DHARs leadership and MTF/DTF POC will submit, in a timely matter, information necessary to comply with reporting requirements mandated by any oversight body or DPCLFD, as needed, to complete the semi-annual Section 803 Report in accordance with Reference (l).

b. Records Management. DHA personnel will adhere to applicable retention, access, and disposition policies regarding Civil Liberties complaints arising within the DHA and maintain supporting documents in accordance References (f) and (aj).

c. Markets, SSO, DHARs and MTFs/DTFs in receipt of Civil Liberties complaints will forward the initial complaints immediately or no later than two business days to the DHA National Capital Region PCL Mailbox DHA Civil Liberties Mailbox at: dha.ncr.pcl.mbx.dha-civil-liberties-mbx@health.mil for intake, coordination, and review.

9. PRIVACY COMPLIANCE REVIEWS. Pursuant of References (h), (i), (l), and (m), the DHA is required to safeguard PII and PHI. Also, in accordance with Reference (j), the DHA PCLO is responsible for conducting periodic technical and non-technical assessments of the potential risks and vulnerabilities with respect to the confidentiality, integrity, and availability of the ePHI that is owned or managed by DHA. Markets, SSO, DHARs, and MTFs will conduct annual compliance reviews of their facility to ensure compliance with the HIPAA & Privacy Act policies, rules, and regulations.

a. CRA. Annually, DHA PCLO will conduct CRA reviews of a representative sample of DHA Program Offices, Markets, SSO, DHARs, and MTFs/DTFs. CRA reviews consist of a foundational questionnaire designed to assess compliance with regulatory requirements. Interviews with appropriate staff tailored to gauge privacy compliance posture and identify gaps and opportunities for compliance assistance. Upon completion of a CRA, a Final CRA Initiative Report will be provided to include key findings and recommendations for improved privacy compliance.

b. HIPAA Security Risk Assessment

(1) At least annually, DHA PCLO personnel, or assigned contractors, will conduct three assessments: Technical Security Evaluation, Non-Technical Security Evaluation, and Risk Analysis, that, when combined, will form the HSRA HIPAA Privacy and Security Compliance Risk Assessment Final Report involving the DHA Components.

(2) The final report will be made available to DHA leadership and workforce members for heightened awareness.

c. Privacy Risk Management within RMF Plan

(1) The DHA PCLO will review the Plan involving the DHA Components on a quarterly basis for updates.

(2) Privacy Risk Management within RMF changes will be communicated via the methods described within the Communications Plan.

d. Compliance Audits

(1) System owner will ensure internal controls are properly implemented and audits of data access are conducted to detect and deter any breach of PII/PHI and report findings to PCLO and RMED as applicable.

(2) MTF/DTF HPO/HSO will ensure procedures are adopted consistent with RMF control requirements for regular review of IS that process PII/PHI.

10. COMPLIANCE REPORTING. Pursuant to References (g), (h), (q), (v) through (x), and (p), the DHA PCLO will issue data calls to the DHA along with accompanying guidance to meet its reporting requirements.

a. The DHA Headquarters CPO works with the DHA Directors to report on what Office of Management and Budget determines to be the priority activities for reporting.

b. The DHA Headquarters Senior Information Security Officer provides DHA PCLO, in collaboration with the CPO, Privacy Program metrics and related information required to meet the organization's privacy reporting requirements, in accordance with References (t) and (u).

c. MTF/DTF HPOs/HSOs will assist the DHA PCLO with Compliance reporting.

d. The DHA Headquarters CPO also provides input for the Section 803 Reporting twice a year, in accordance with Reference (l), in March and September, chiefly focusing on whether complaints in those areas were received by the component, and if so, how they were resolved.

e. The DHA PCLO will develop and publish reporting templates and guidelines for use by the MTFs/DTFs.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	Action Officer
CIO	Chief Information Officer
CPO	Chief Privacy Officer
CRA	Compliance Risk Assessment
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
DPCLFD	Defense Privacy, Civil Liberties, and Freedom of Information Act Directorate
DSA	Data Sharing Agreement
DSAA	Data Sharing Agreement Application
DTF	dental treatment facility
ePHI	Electronic Protected Health Information
FOIA	Freedom of Information Act
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Health Information Privacy and Security
HIPSCC	Health Information Privacy & Security Compliance Committee
HPO	HIPAA Privacy Officer
HSO	HIPAA Security Officer
IMCO	Information Management Control Office
IRB	Institutional Review Board
IS	Information Systems
IT	Information Technology
JKO	Joint Knowledge Online
MHS	Military Health System
MTF	Military Medical Treatment Facility
OCR	Office of Civil Rights
OSD	Office of Secretary of Defense
PAR	Privacy Assessment Report
PCLO	Privacy and Civil Liberties Office
PHI	Protected Health Information

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POC	Point of Contact
PMET	PCLO's Monthly Education and Training
RFI	Request for Information
RMED	Risk Management Executive Division
RMF	Risk Management Framework
SAOP	Senior Agency Official for Privacy
SCOP	Senior Component Office for Privacy
SOR	System of Record
SORN	System of Records Notice
SSN	Social Security Number

PART II. DEFINITIONS

breach or DoD breach. As defined in Reference (ah), the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII; or (2) an authorized user accesses or potentially accesses PII for any other than authorized purpose.

business associate. With respect to a DoD covered entity, a party that creates, receives, maintains, or transmits PHI on behalf of the DoD covered entity for a function or activity regulated by this issuance; or a party that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such DoD covered entity, where the provision of the service involves disclosure of PHI to that party. A DoD or other covered entity may be a business associate performing HIPAA-covered functions on behalf of another DoD covered entity. A more detailed definition is provided in Reference (h).

covered entity. A health plan, or a health care provider who transmits any health information in electronic form in connection with a standard transaction. A more detailed definition is provided in Reference (h).

dental treatment facility. Established for the purpose of furnishing dental care to eligible individuals.

disclosure. In compliance with HIPAA, it is the release, transfer, provision of access to, or other divulging in any manner of PHI outside the entity holding the information. For purposes of the Privacy Act, the term "disclosure" is "the transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government Agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian", see Reference (k).

DoD covered entity. In the case of a health plan administered by DoD, the DoD Component (or subcomponent) functions as the administrator of the health plan. To the extent this issuance prescribes duties to be performed by covered entities, the term refers only to DoD covered entities. All covered entities within the MHS (including both health plans and health care providers) are DoD covered entities and designated as a single covered entity. Not all healthcare providers affiliated with the Military Services are DoD covered entities; among those who are not are:

Providers associated with military entrance processing stations or DoD medical examination review boards.

Reserve Components practicing outside the authority of military treatment facilities that do not engage in electronic standard transactions covered by this issuance.

A more detailed definition is provided in Reference (h).

HIPAA or Privacy Act complaint. A written statement submitted to a DoD covered entity's HIPAA Privacy Officer or to the HHS OCR alleging that the DoD covered entity has violated an individual's health information privacy rights or committed a violation of the HIPAA Privacy or Security Rule provisions.

HIPAA Privacy Officer. The member of the workforce of a DoD covered entity who is the designated point of contact for the DoD covered entity for handling HIPAA/Privacy Act complaints. Such workforce member may be a member of a Military Service, a DoD civilian employee, or a contractor of the DoD covered entity or component. As stated in paragraph 4.b. of Enclosure 2, a DoD covered entity's HIPAA Privacy Officer may also be the designated HIPAA Security Officer for that DoD covered entity.

HIPAA Security Officer. The member of the workforce of a DoD covered entity who is the designated POC for the DoD covered entity responsible for the development, implementation, maintenance, oversight, and reporting of security requirements for ePHI. Such workforce member may be a member of a Military Service, a DoD civilian employee, or a contractor of the DoD covered entity. As stated in paragraph 4.b. of Enclosure 2, a DoD covered entity's HPO may also be the designated HSO for that DoD covered entity.

Military Health System. All DoD health plans and all DoD healthcare providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by, the DHA, the Surgeon General of the Army, the Surgeon General of the Navy, or the Surgeon General of the Air Force.

Military Medical Treatment Facility. As in section (g)(3) of Reference (e): (A) any fixed facility of the DoD that is outside of a deployed environment and used primarily for health care; and (B) any other location used for purposes of providing health care services as designated by the Secretary of Defense.

Personally Identifiable Information. Defined in Reference (y). Under Reference (k), PII is information about an individual that identifies, links, relates, or is unique to or describes the individual (e.g., a SSN, age, military rank, civilian grade, marital status).

Privacy Act of 1974. A federal statute, codified in Reference (l), that, among other things, protects the confidentiality of federal records maintained on individuals. In contrast to HIPAA, applicability of the Privacy Act is limited to the federal government.

Protected Health Information. Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a DoD covered entity in its role as employer. PHI is a subset of PII, with respect to living persons (g).

Senior Component Official for Privacy. A member of the senior executive service or general officer/flag officer acting on behalf of the Senior Agency Official for Privacy and responsible for the overall implementation of the Privacy and Civil Liberties programs in their DoD or OSD Component.

System of Records Notice. The term SORN defined and referenced in Reference (l) means the notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in this Circular. As explained in Reference (l), a SORN may be comprised of a single Federal Register notice addressing all the required elements that describe the current system of records, or it may be comprised of multiple Federal Register notices that together address all the required elements.