Privacy Program Plan

DHA PRIVACY AND CIVIL LIBERTIES OFFICE

Version 1.6

Sep 25, 2019

Document Change Control

The signature of the Chief, DHA Privacy Office, formally issues this DHA Privacy Program Plan.

Version	Release Date	Summary of Changes	Issuer	Signature
Version 1.0	November 2, 2017	Initial Release	Chief, DHA Privacy Office	
Version 1.1	Feb 2, 2018	Update after quarterly review	Chief, DHA Privacy Office	
Version 1.2	Mar 15, 2018	Updated PPP review frequency	Acting Chief, DHA Privacy Office	
Version 1.3	July 17, 2018	Signature block for Acting Chief	Acting Chief, DHA Privacy Office	
Version 1.4	Sep 5, 2018	Signature block for Acting Chief	Acting Chief, DHA Privacy Office	
Version 1.5	Sep 19, 2018	Update after semi-annual review	Acting Chief, DHA Privacy Office	
Version 1.6	Mar 27, 2019	Update after semi-annual review	Chief, DHA Privacy Office	
Version 1.6	Sep 25, 2019	Semi-Annual review	Chief, DHA Privacy Office	KELETA.RAHWA.AMDEMARIAM.1298456431 Digitally signed by KELETA.RAHWA.AMDEMARIAM.1298456431 Date: 2019.09.25 10:55:55 -04'00'

Table of Contents

1.0 Executive Summary 1
1.1 Purpose and Scope of the DHA Privacy Program Plan 1
1.2 Authority 2
2.0 Background 4
3.0 Privacy Program Primary Roles and Responsibilities 6
3.1 DHA Privacy Office Roles and Responsibilities 7
3.1.1 DHA Privacy Office and its Chief Privacy Officer (CPO) 7
3.1.2 DHA Data Sharing Compliance Manager 8
3.1.3 DHA FOIA Manager 8
3.1.4 DHA HIPAA Compliance Manager 8
3.1.5 DHA Federal Privacy Compliance Manager 9
3.2 DoD and DHA Officials, Key Roles, and Offices 10
3.2.1 Senior Agency Official for Privacy (SAOP) 10
3.2.2 DoD Chief Information Officer (CIO) 10
3.2.3 DHA CIO 10
3.2.4 DHA CSOP 10
3.2.5 DHA Chief Information Security Officer (DHA CISO) 11
3.2.6 Program Managers 11
3.2.7 Information System Owners 11
3.2.8 DHA Workforce 11
3.2.9 Program Integration Office 11
3.2.10 DHA's MHS Communications Office 12
3.2.11 Office of the General Counsel (OGC) 12
3.2.12 Records Management Office 12
4.0 Privacy Program Foundational Principles 12
5.0 Federal Agency Privacy Compliance 13
5.1 Privacy Act of 1974 14
5.1.1 Systems of Records Notices 14
5.1.2 Privacy Act Statements 15
5.1.3 Computer Matching Agreements (CMA) Program 15

5.1.4 SSN Use, Reduction, and Elimination Program 16
5.1.5 Privacy Considerations for Contracts and Interagency Agreements 17
5.2 E-Government Act of 2002 (Section 208 and FISMA) 17
5.2.1 Privacy Threshold Analysis 18
5.2.2 PIAs 18
5.2.3 Privacy Notice 19
5.2.4 Inventory of Personally Identifiable Information 19
5.2.5 Annual Reporting on Compliance 20
5.2.6 Training in IT Security and Privacy 20
5.3 Paperwork Reduction act (PRA) 21
6.0 HIPAA 21
6.1 General Overview 21
6.2 DoD's Organizational Structure Under HIPAA 23
6.3 HIPAA Compliance Within DoD 23
6.3.1 Designation of a HIPAA Privacy/Security Officer 24
6.3.2 Workforce Training 24
6.3.3 Policy Development and Review 24
6.3.4 Use and Disclosure Notice 24
6.3.5 Complaints 24
6.3.6 Sanctions 25
6.3.7 Business Associate Agreements 25
6.3.8 Breach Response and Notification 25
6.3.9 Safeguards 25
6.3.10 HIPAA Privacy and Security Risk Management 26
6.3.11 Individual Rights 26
7.0 Data Sharing 27
7.1 Data Sharing Agreement Applications 27
7.2 Data Evaluation Workgroup (DEW) 27
7.3 DHA HIPAA Privacy Board 28
7.4 SSV Reviews 29
7.5 DSA 29

8.0 FOIA 30
8.1 FOIA Disclosure Limitations 30
9.0 Civil Liberties 30
10.0 Breach Prevention and Response 31
10.1 Breach Response 31
10.2 Privacy Incident Response Plan 32
10.3 Tracking Privacy Incidents 33
10.4 Contingency Planning 33
10.5 Managing Privacy Complaints and Redress 34
11.0 Privacy and Cybersecurity Information Life Cycle Management 34
11.1 Role of Privacy in Information Life Cycle Management 34
11.2 Role of Security in Information Life Cycle Management 35
11.3 Privacy and Security Controls Working to protect PII and PHI in new or emerging technology 39
12.3.1 Encryption as an Automated Privacy Control 39
12.3.2 Cloud Computing 39
12.3.3 Data-Loss-Prevention (DLP) 39
12.0 Privacy Training and Awareness 40
12.1 Mandatory Training 40
12.2 Role-based Training 41
12.3 Training Delivery System 44
13.0 Reporting Requirements 44
13.1 Breach Reporting 44
13.2 Section 803 Reporting 45
13.3 Internal Reporting 45
14.0 Privacy Consultation 45
14.1 Working Groups 45
14.2 Information Dissemination 46
15.0 Conclusion 46

APPENDIX A: ACRONYMS 48
APPENDIX B: STATUTES AND REGULATIONS 51
APPENDIX C: DEFINITIONS 53
APPENDIX D: TABLE OF REQUIREMENTS 57
APPENDIX E: CNSS 1253 PRIVACY CONTROLS MAPPING 59

LIST OF TABLES

TABLE 1: FEDERAL LAWS AND DOD REGULATIONS 2
TABLE 2: DHA PRIVACY PROGRAM COMPONENTS 5
TABLE 3: PRIVACY CONTROL IMPLEMENTATION 36
TABLE 4: DHA PRIVACY OFFICE TRAININGS 42

1.0 Executive Summary

11 PURPOSE AND SCOPE OF THE DHA PRIVACY PROGRAM PLAN

The Defense Health Agency (DHA) is a federal combat support agency whose mission is to lead the Military Health System (MHS) integrated system of readiness and health to deliver the Quadruple Aim: increased readiness, better health, better care, and lower cost. One means to achieve such goals is to optimize critical internal management processes, which includes compliance with relevant statutes, regulations, and guidance. Compliance with privacy requirements is a key element of such optimization.

As a component within the Department of Defense (DoD), DHA is a federal agency for purposes of compliance with the Privacy Act and related legislation. In addition, DHA is a covered entity (CE) under the Health Insurance Portability and Accountability Act (HIPAA) by virtue of managing the TRICARE Health Plan for United States Armed Forces, their families and retirees, and housing healthcare providers within the National Capital Region Medical Directorate, such as Walter Reed National Military Medical Center. Therefore, the DHA Privacy and Civil Liberties Office (Privacy Office) must manage privacy requirements for both federal agency privacy in general and HIPAA privacy.

In addition, as the National Defense Authorization Act (NDAA) modifications to the structure of the MHS targeted for October 1, 2018 take shape, the DHA Privacy Office can be expected to accrue an increasingly larger role in streamlining and managing processes related to privacy across the MHS. Therefore, in addition to meeting current DHA Privacy Office requirements, the DHA Privacy Office also needs to engage in strategic planning in full collaboration with the Services to optimize the opportunities and challenges ahead. This Privacy Program Plan (PPP) therefore serves as a living document which will be updated when warranted and will be reviewed semi-annually.

The DHA Privacy Office has developed this PPP to present its strategic concept of operations, including descriptions of how DHA complies with federal privacy requirements and related information management subject areas.

This DHA PPP formally documents the DHA's Privacy Program, including a description of the structure of the Privacy Program, the subject programs and activities that comprise the program, the roles and responsibilities of privacy officials and staff, the strategic goals and objectives of the Privacy Program, and the controls in place or planned – such as policies and procedures and specific programs and activities for meeting applicable privacy requirements and managing privacy risks.

This PPP reflects the DHA Privacy Office's unique responsibilities within the DoD's organizational structure under the leadership of DHA Resources and Management Directorate led by the DHA Component Senior Official for Privacy (CSOP), and under additional oversight of the Defense Privacy and Civil Liberties and Transparency Division (DPCLTD), which has responsibility for coordinating and guiding all DoD component Privacy Offices. This document is intended to support the management of information as a strategic resource, including reduction of risk to the organization and the Government in promoting and implementing privacy protections, and evidences DHA's compliance strategy.

1.2 AUTHORITY

The following listing of laws and regulations establish the requirements of a comprehensive Privacy Program.

Table 1: Federal Laws and DoD Regulations

Laws and Regulations	Impact
Privacy Act of 1974	The Privacy Act of 1974 protects the privacy of individuals by establishing "Fair Information Practices" for the collection, maintenance, use, and dissemination of information by federal agencies.
DoD Directive (DoDD) 5400.11 and DoD 5400.11-R, DoD Privacy Program	Establishes policies and procedures for the DoD Privacy Program based on the Privacy Act of 1974.
DoD Instruction (DoDI) 1000.30, Reduction of Use of Social Security Numbers (SSNs) in DoD	Establishes policy and assigns responsibility for SSN reduction in DoD.
E-Government (E-Gov) Act of 2002	Section 208 of the E-Gov Act requires federal agencies to conduct Privacy Impact Assessments (PIAs) before developing or procuring information technology (IT) systems that collect, maintain, or disseminate personally identifiable information (PII).
DoDI 5400.16, DoD PIA Guidance	Provides procedures for the completion and approval of PIAs in DoD.
Federal Information Security Modernization Act (FISMA) of 2002	Title III of the E-Gov Act, known as FISMA, superseded and made permanent some of the provisions of the Government Information Security Reform Act of 2000. FISMA outlines key security standards and guidelines related to the management of information systems by federal agencies.
Health Insurance Portability and Accountability Act	The HIPAA Privacy Rule establishes rules around the use and disclosure of protected health information (PHI), while the HIPAA Security Rule provides a series of administrative, physical, and technical safeguards, to address technical and non-technical shifts in the organization's protection of electronic PHI.

DoD 6025.18-R, DoD Health Information Privacy Regulation	Establishes DoD's implementation of the HIPAA Privacy Rule.
DoDI 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs	Establishes DoD's implementation of the HIPAA Security Rule.
National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations	Standardized set of management, operational, and technical controls and safeguards and a Risk Management Framework (RMF).
NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	Provides guidance for federal agencies to ensure that certain types of federal information are protected when processed, stored, and used in non-federal information systems.
Office of Management and Budget (OMB) Circular A-130: Management of Federal Information Resources	OMB Circular A-130, requires agencies to implement security requirements to protect personal information in automated information systems and provides specific guidelines for implementing these requirements, including a minimum set of controls for federal automated information programs.
DoDI 8500.01, Cybersecurity	Establishes a DoD cybersecurity program to protect and defend DoD information and IT and adopts the term "cybersecurity" to be used instead of the term "information assurance."
DoDI 8510.01, RMF for DoD IT	Establishes the RMF for DoD IT, cybersecurity policy, and assigns responsibilities for executing and maintaining RMF.
Committee on National Security Systems (CNSS) Privacy Overlays	Identifies security and privacy control specifications required to protect PII/PHI in a National Security System (NSS) and reduce privacy risks to individuals throughout the information lifecycle.
Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004	Identifies intelligence community and the intelligence related activities of the United States Government, including requirements to protect privacy of citizens while establishing the Information Sharing Environment.
DoDI 1000.29, Civil Liberties Program	Establishes policy and assigns responsibilities for the implementation of the DoD Civil Liberties Program.

2.0 Background

The DHA is a joint, integrated Combat Support Agency that enables the Army, Navy, and Air Force medical services to provide a medically ready force to Combatant Commands in both peacetime and wartime. The DHA supports the delivery of integrated, affordable, and high-quality health services to MHS beneficiaries and is responsible for driving greater integration of clinical and business processes across the MHS. Established October 2013, the idea of the DHA stemmed from a long-held conviction that military health care could be better integrated and more efficient. With the Presidential signing of the 2017 NDAA, the DHA is poised to take an even greater role in military health and requires increased collaboration across the MHS and the Services after October 1, 2018.

In further support of the QUAD goals, NDAA Section 702 requires the DHA to act as a single agency responsible for the administration of all Military Treatment Facilities (MTFs). As such, the DHA Privacy Office began the planning process to assume management responsibility for the privacy and security functions of MTFs on October 1, 2018. The DHA Privacy Office drafted and received approval on the DHA J-1 Privacy Workstream Proposal, and as a result facilitated regularly scheduled Privacy FC Workgroup (FCWG) meetings with Service representatives to lay the groundwork for developing a comprehensive implementation plan covering the management of privacy compliance functions. Each of the Services and the MTFs deliver various levels of privacy and security support. In some instances, the specific activities associated with each privacy and security function may differ. Also, the Services historically had the option of abiding by policies developed by the DHA Privacy Office or developing Service-specific policies. The Services were also able to work independently on privacy issues or collaborate with the DHA Privacy Office. Therefore, the current state reflects a mixture of DHA-level policies, Service-level policies, and MTF-level procedures. However, going forward and in accordance with NDAA 702, the MTFs will follow DHA Privacy Office policies.

The DHA Privacy Office oversees the protection of PII and PHI within the MHS. As the MHS has grown to one of the largest integrated healthcare delivery systems in the United States, so have the responsibilities of the DHA Privacy Office. The DHA Privacy Office supports MHS compliance with Federal privacy and security laws, and DoD regulations and guidance. This includes managing and evaluating potential risks and threats to the privacy and security of MHS health data by performing critical reviews through:

- Evaluation of privacy and security safeguards, including conducting annual HIPAA

Security Risk Assessments;

- Performance of Internal DHA Privacy Office Compliance Assessments;
- Establishment of organizational performance metrics to identify and measure potential compliance risks; and
- Consultation for leadership and the workforce on areas of DHA-level oversight.

In addition, the DHA Privacy Office has specific responsibility for various DHA-level areas. The DHA Privacy Office supports activities related to compliance with Federal laws, DoD regulations, and guidelines governing the privacy and security of PII/PHI. The DHA Privacy Program includes component policies, procedures, programs and activities that implement the requirements of applicable privacy laws, regulations, and guidance, as captured in Table 2. These program components are addressed in detail throughout this PPP.

Table 2: DHA Privacy Program Components

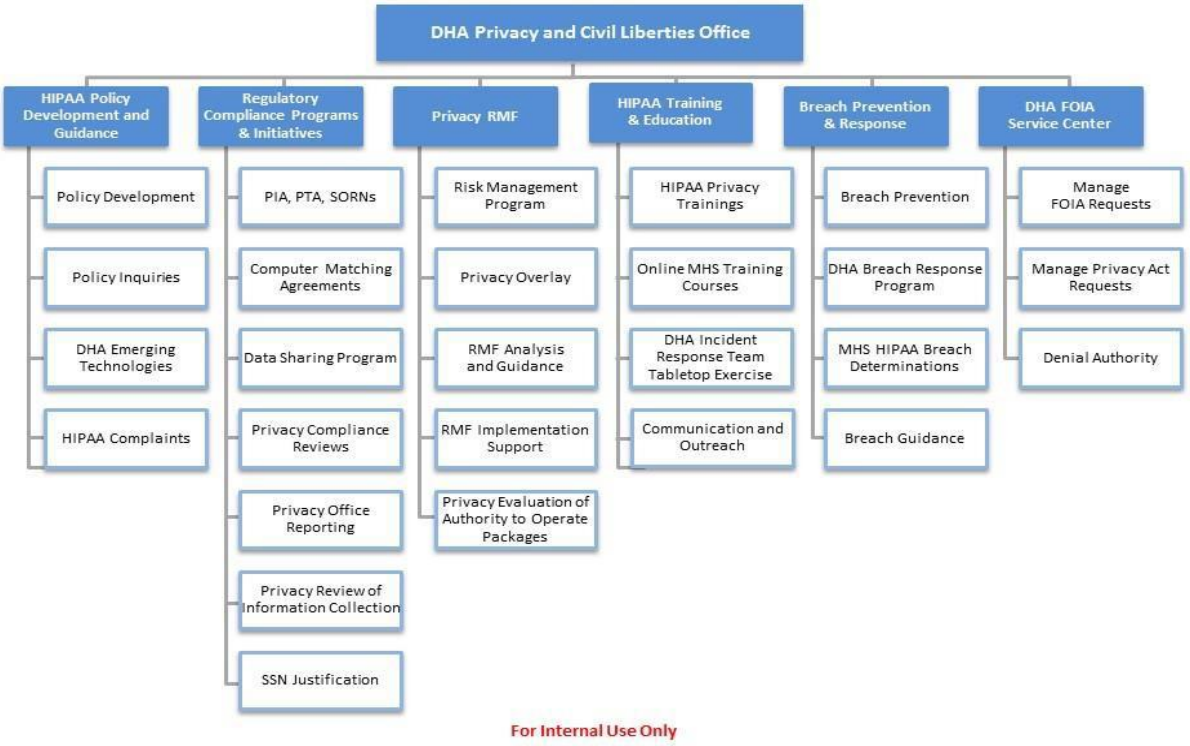
Federal Agency Privacy Compliance	DHA Privacy Office provides policy and procedural guidance and oversees DHA implementation of the Privacy Act of 1974, Section 208 of the E-Gov Act, parts of FISMA, and the Paperwork Reduction Act. In creating policies and providing guidance, DHA Privacy Office incorporates the guidance provided by OMB and NIST.
HIPAA	DHA Privacy Office helps MHS comply with the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rule. In addition, the DHA Privacy Offices investigates and prepares responses to HIPAA complaints either received directly or through the Department of Health and Human Services (HHS).
Data Sharing	DHA Privacy Office reviews and approves Data Sharing Agreements to ensure that data is shared appropriately when it is DHA managed or owned data that is being requested.
Freedom of Information Act (FOIA)	DHA Freedom of Information Service Center has principal authority to ensure Health Affairs (HA), DHA, and its components are in full compliance with FOIA and processes their FOIA requests.
Civil Liberties	DHA Privacy Office supports compliance with civil liberties laws, and related DoD issuances, by providing training, adjudicating civil liberties complaints, and adhering to other program requirements.
Breach Prevention and Response	DHA Privacy Office coordinates breach reporting

	within the MHS.
Privacy and Cybersecurity Information Lifecycle Management	DHA Privacy Office manages and evaluates potential risks and threats to the privacy and security of MHS health data by performing critical reviews.
Privacy Training and Awareness	DHA Privacy Office is responsible for the development and availability of a HIPAA and Privacy Act training course and other onsite and online training offerings.
Reporting Requirements	DHA Privacy Office maintains compliance with regulatory reporting requirements including FISMA, Section 803 reporting, FOIA and Breach reporting.
Privacy Consultation	DHA Privacy Office provides subject matter expertise on a wide range of privacy and security issues to various stakeholders including work groups, senior management, program offices, and the Services upon request.

3.0 Privacy Program Primary Roles and Responsibilities

Protecting privacy is the mission of the DHA Privacy Office. Privacy stewardship and governance are keys to a successful Privacy Program. The DHA Privacy Office considers privacy implications when developing and reviewing policy and in making program decisions about business operations, application development, and related activities. To successfully protect PII/PHI, DHA officials and employees work daily to implement the policies and program requirements into their program functions and activities. The following outlines the roles and general responsibilities for implementing the DHA Privacy Program.

The mission of the DHA Privacy Office, under the direction of DHA's Administration and Management Directorate, is to oversee the protection of PII/PHI within the MHS. The MHS is one of the largest integrated healthcare delivery systems within the United States, serving over 9.4 million eligible beneficiaries around the world. The DHA Privacy Office supports MHS compliance with federal privacy, HIPAA, and DoD regulations and guidelines. Each core program within the DHA Privacy Office are identified below.



3.1 DHA PRIVACY OFFICE ROLES AND RESPONSIBILITIES

3.1.1 DHA Privacy Office and its Chief Privacy Officer (CPO)

The DHA Privacy Office is led by its Chief, who serves as the DHA CPO, as well as the DHA HIPAA Privacy Officer and DHA HIPAA Security Officer. This Chief reports to DHA's CSOP, who directs the Resources and Management Directorate, J1-J8. The DHA Privacy Office, oversees the protection of PII and PHI within the DHA, and to some extent the MHS, and is responsible for implementing the DHA Privacy Program. This is accomplished through specific sections of the DHA Privacy Office, and through the creation of governance documents in the form of policies and procedures. As part of oversight for the Privacy Office programs, the Chief also serves as the DHA FOIA Liaison and the DHA Civil Liberties Officer. The DHA Privacy Office also has lead responsibility for developing compliance documentation; privacy awareness training; privacy incident analysis and privacy breach responses; and coordinating with DHA officials and employees on privacy protection and compliance activities. The DHA Privacy Office works

collaboratively with other DHA Joint Staff Directors, the Services, DoD components, and other agencies when needed.

The CPO:

(1) Manages DHA privacy and related compliance activities;
(2) Reviews applicable DHA privacy artifacts including system of records notices (SORNs), PIAs; privacy threshold analysis (PTAs), Privacy Act Reviews, data sharing agreements, etc.;
(3) Represents privacy in RMF implementation; and
(4) Oversees training, reporting, and consultation requirements.

3.1.2 DHA Data Sharing Compliance Manager

Serves as the DHA Data Sharing Compliance Manager responsible for conducting an effective and efficient compliance review of Data Sharing Agreements and Computer Matching Agreements submissions from external federal partners and directorates within the DHA.

The DHA Data Sharing Compliance Manager:

(1) Provides quality oversight and management to the Data Compliance Program.
(2) Guides and manages the Data Sharing Agreement (DSA) team to meet the needs of the demand by conducting an efficient and thorough analysis of the Data Sharing Agreement Application (DSAA).
(3) Provides expertise and general support of the organizational Privacy Office for major issues that may impact DHA Data Sharing program.

3.1.3 DHA FOIA Manager

Serves as the DHA FOIA Officer. Assists the Chief of the DHA Privacy Office with management of daily operations of the FOIA Service Center for DHA. This Service Center, housed within the DHA Privacy Office, receives and responds to DHA FOIA requests, receives and responds to DHA Privacy Act requests, tracks and manages FOIA processing efforts, and coordinates with FOIA Points of Contact through the agency organization in order to receive responsive records. The DHA FOIA Manager is also responsible for associated training, guidance, and reporting requirements.

3.1.4 DHA HIPAA Compliance Manager

Assists the Chief of the DHA Privacy Office with duties relating to serving as the HIPAA Privacy Officer and the HIPAA Security Officer for DHA. The DHA HIPAA Compliance

Manager coordinates breach response efforts and oversees the reporting and remediation efforts of breaches within the MHS.

The DHA HIPAA Compliance Manager:

(1) Provides consultation on HIPAA Privacy and Security Rule implementation questions from MHS workforce members and TRICARE beneficiaries.
(2) Processes, coordinates, and analyzes investigations of HIPAA Privacy complaints concerning allegations within the MHS (complaints are filed directly by beneficiaries or received from the HHS Office for Civil Rights).
(3) Ensures requests for the MHS the Notice of Privacy Practices are fulfilled and available to patients at MHS facilities.
(4) Provides information and guidance to the Armed Services, TRICARE Program Offices, and Managed Care Support Contractors regarding the HIPAA Privacy and Security Rules.
(5) Conducts an annual risk assessment on HIPAA Security compliance for the DHA.
(6) Leads the DHA Compliance Risk Assessment Initiative which is aimed at gauging the compliance posture of DHA offices as it pertains to Privacy Act and HIPAA compliance.
(7) Assists in the planning and facilitation of HIPAA and Breach Response training for all MHS workforce members.
(8) Issues guidance and leads drafting efforts for HIPAA compliance related policies, procedures, and administrative instructions.
(9) Coordinates breach response efforts and oversees the reporting and remediation efforts of breaches within the MHS.
(10) Provides accurate and timely responses to breach-related inquiries from MHS workforce members and TRICARE beneficiaries.
(11) Identifies, analyzes, and reports all MHS breaches reportable to HHS in accordance with Health Information Technology for Economic and Clinical Health (HITECH)/HIPAA.

3.1.5 DHA Federal Privacy Compliance Manager

Assists the Chief of the DHA Privacy Office with duties relating to compliance with the Privacy Act, the E-Government Act, Federal Information Security Management Act, National Institute of Standards and Technology privacy guidance, Office of Management and Budget privacy guidance for executive agencies, and related regulations and guidance. Such responsibilities therefore include system of records notices, privacy impact

assessments for electronic systems, Privacy Act statements, and associated guidance, training, consultation, and reporting requirements.

3.2 DOD AND DHA OFFICIALS, KEY ROLES, AND OFFICES

3.2.1 Senior Agency Official for Privacy (SAOP)

The SAOP within the Office of the Secretary, DoD, has overall responsibility and accountability for ensuring DoD's (including DHA's) implementation of privacy protections, including issuance of guidance, for full compliance with federal laws, regulations, and policies relating to privacy.

3.2.2 DoD Chief Information Officer (CIO)

The DoD CIO is the Principal Staff Assistant and senior advisor to the Secretary of Defense for IT (including national security systems and defense business systems), information resources management and efficiencies. The DoD CIO is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; DoDD 5144.02, November 21, 2014 cybersecurity; positioning, navigation, and timing policy; and the DoD information enterprise that supports DoD command and control.

3.2.3 DHA CIO

The DHA CIO is the leader of all matters regarding IT at DHA, including overseeing the authority to operate process for IT systems, and being the final reviewing official for PIAs. Under the shared services setup at DHA, the DHA CIO has some level of responsibility for the infrastructure of the entire Military Health System, providing oversight and guidance on how it is to be operated and maintained.

3.2.4 DHA CSOP

The DHA CSOP has component responsibility and accountability for implementation of information privacy protections, and provides oversight of each component's compliance efforts including review of the component's privacy policies and procedures, adequate resourcing for privacy protection and risk reduction, and for RMF responsibilities in authorizing and accrediting IT systems. Under DoD's organizational structure, the DHA CSOP is designated at the DHA level. Each CSOP conducts the agency level privacy compliance responsibility and thus supports the overall mission of the DoD level SAOP. Some of the day to day responsibilities in support of this role can be appropriately delegated to the CPO.

3.2.5 DHA Chief Information Security Officer (DHA CISO)

The head of the Health Information Technology (HIT) Cybersecurity Division is responsible for reviewing and approving system security plans of IT systems, for assisting the DHA CIO with policies and procedures relating to cyber security, and for reviewing and approving PIAs from the cybersecurity area of expertise.

3.2.6 Program Managers

Program Managers are responsible for ensuring privacy and security of the PII that their programs collect, use, maintain, and disseminate and for complying with federal privacy authorities.

3.2.7 Information System Owners

Information System Owners are responsible for ensuring the privacy and security of the PII that their information systems collect, use, maintain, and disseminate and for complying with federal privacy authorities. Information System Owners are responsible for the overall procurement, development, integration, maintenance, secure operation, and safeguarding of information including PII for their information system(s). System Owners must file a SORN, if applicable, and must complete the entire Federal Register review period before the system will be permitted to operate in the production environment. System Owners must also submit documentation for a new or revised System of Records (SOR) or if there are changes to existing SORs to DHA Privacy Office for processing.

3.2.8 DHA Workforce

DHA workforce (employees and contractors) are responsible for complying with the requirements of the Privacy Act and other federal privacy authorities, which require employees and contractors to protect from unauthorized exposure the PII entrusted to their care, to complete privacy compliance activities, to report breaches of PII, and to reduce the volume and types of PII to only that needed for program functions. They are also responsible for successfully completing the required HIPAA/Privacy training for the workforce currently on the Joint Knowledge Online (JKO) platform.

3.2.9 Program Integration Office

The Program Integration Office aids with posting privacy policies on all DHA websites, explaining that visitors are being directed to a non-government website, and branding and marking the DHA presence on third-party websites.

3.2.10 DHA's MHS Communications Office

The DHA's MHS Communications Office is responsible for DHA strategic communications such as press releases, guidance for call centers, etc. They also aid with posting privacy policies on all DHA websites, providing notices when users are being directed to a non-government website, and with branding and marking the DHA presence on third party websites.

3.2.11 Office of the General Counsel (OGC)

OGC interprets privacy statutes, regulations, and other legal authorities and provides guidance whenever needed. They also review reports, proposed rules, other significant submissions, and collaborate on FOIA responses. Additionally, OGC provides staffing for reviewing DHA FOIA administrative appeals.

3.2.12 Records Management Office

The Records Management Office supports all HA/DHA components to ensure proper maintenance, use, and disposition of paper and electronic records, in accordance with federal laws, regulations, TRICARE Management Activity (TMA) Records Retention Schedule, and DoD guidance regarding the protection of sensitive information.

4.0 Privacy Program Foundational Principles

The DHA Privacy Office supports and seeks to implement the Fair Information Practice Principles (FIPPs), the foundation of many federal privacy laws. The FIPPs formed the basis for the Privacy Act, the E-Gov Act Section 208, and the OMB privacy policies applicable to all federal agency information systems and organizations. It was also foundational to many of the core principles in HIPAA. The DHA Privacy Program adheres to the following FIPPs and uses them as a guide for establishing policies and procedures that address privacy protections in DHA programs throughout the information life cycle.

a. **Authority and Purpose:** Articulate specifically the authority that permits the collection of PII and articulate specifically the purposes and intent of PII use.
b. **Accountability, Audit, and Risk Management:** Provide accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern collection, use, maintenance, and dissemination of PII; and audit for the actual use of PII to demonstrate compliance with established privacy controls.

c. **Data Quality and Integrity:** Ensure, to the greatest extent possible, that PII use is accurate, relevant, timely, and complete, as identified in the public notice.
d. **Data Minimization and Retention:** Only collect PII that is directly relevant and necessary to accomplish the specified purposes and only retain PII for as long as necessary to fulfill the specified purposes and in accordance with the appropriate National Archives and Records Administration (NARA)-approved record retention schedule.
e. **Individual Participation and Redress:** Involve the individual in the decision-making process regarding the collection and use of his or her PII and seek individual consent for the collection, use, maintenance, and dissemination of PII; and provide a mechanism for appropriate access and amendment of the PII.
f. **Security:** Protect PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks, such as: loss, unauthorized access or use, destruction, modification; or unintended or inappropriate disclosure.
g. **Transparency:** Provide notice to the individual regarding the collection, use, maintenance, and dissemination of PII.
h. **Use Limitation:** Use PII solely for the purposes specified in the public notice and share information compatible with PII intent and objectives.

5.0 Federal Agency Privacy Compliance

All federal executive branch agencies, whether a CE under HIPAA or not, must comply with general federal privacy requirements. These are chiefly mandated by the Privacy Act of 1974 and the E-Gov of 2002, as well as associated regulations and guidance from OMB and NIST. DoD and DHA have published official policies and procedures implementing the requirements of these laws, regulations, and guidance, including the mandated privacy practices and compliance documentation, such as: privacy risk analysis, PTAs, PIAs, SORNs, Privacy Act Statements, and computer matching agreements. A summary of the required compliance documentation and record maintenance guidance is provided in a table in Appendix D: Table of Requirements.

By implementing the key tools for privacy compliance – the PTAs, PIAs, and SORNs – the DHA identifies holdings of PII, assesses privacy risks, and implements privacy protections into the life cycle of information management. To ensure that privacy practices and controls are integrated into the DHA's programs and systems, the DHA CPO and DHA Compliance Manager works with program managers, System Owners, and Cybersecurity personnel.

5.1 PRIVACY ACT OF 1974

The Privacy Act mandates that the federal agencies collect and maintain only the PII that is needed to accomplish agency business and ensures that information is accurate, relevant, timely, and complete. The Privacy Act also guarantees rights to individuals whose information is maintained in a system of records, such as the right to notice, consent, access and amendment. A system of records (SOR) is group of information about an individual under the control of an agency from which information is retrieved by an identifier such as name, social security number, or phone number. The Privacy Act also provides individuals the right to receive an accounting of the disclosures of their PII. DoD implemented the Privacy Act requirements in DoD 5400.11-R, *Department of Defense Privacy Program*.

5.1.1 Systems of Records Notices

The Privacy Act applies to SOR, which are DHA-maintained electronic systems or paper files that contain information on individuals ("Privacy Act records"), where the information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. An "individual" includes a citizen of the United States or an alien lawfully admitted for permanent residence. When DHA creates, alters, or deletes a SOR, DHA creates and publishes a SORN in the Federal Register, which notifies the public of the existence, amendment, or deletion of the SOR and provides a description of the character of the SOR. Program Managers and SOR Managers complete SORNs using the SORN template before collecting PII and, thereafter, periodically before making changes to the SOR.

There are three types of SORs: component; department-wide; and government-wide. Component SORs are records created within DHA for its employees or administrative duties or mission and are owned by DHA to cover its internal records. Department-wide SORNs are SOR for which the DoD writes SORNs for the records but may not have physical custody as a matter of necessity. DoD's components may use department-wide SORNs to cover system of records they maintain. Government-wide SORs are records where one Federal agency, such as the Department of Homeland Security, has regulatory authority over records in the custody of multiple agencies, and the agency with regulatory authority publishes a SORN that applies to all of the records regardless of their custodial location. Federal agencies may use government-wide SORNs to cover government-wide SOR.

The DHA Privacy Office assists the Program Managers and SOR Managers in completing the SORN templates and reviews the completed SORN for regulatory requirements. DPCLTD processes the SORN for OMB authorization and Federal Register publication

and notifies Congress following requirements specified in OMB Circular A-108. Once a SORN is published in the Federal Register, it is then posted on http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/DHA-Article-List/.

The SORN must be published before the system becomes operational and revised when any new routine use is adopted by the agency, or other change occurs regarding the system. The DHA Privacy Office coordinates the drafting of the SORN for accuracy and to ensure that it meets the regulatory requirements. The DHA CPO regularly reviews SORNs, including information pertaining to routine uses. The DHA Privacy Office also verifies SORs' compliance by reviewing each Defense Health Program funded information system at least once a quarter. Routine use reviews are conducted in conjunction with the DHA Privacy Office's review of DoD and DHA Forms and PIAs submitted to the DHA Privacy Office. The DHA Privacy Office strives to review each SORN at least every two years to ensure it remains current.

5.1.2 Privacy Act Statements

Pursuant to the Privacy Act and DoD 5400.11-R, when DHA collects an individual's PII for inclusion in an SOR, DHA provides the individual with a Privacy Act statement, regardless of how the PII is collected (paper, electronic, or verbal). The Privacy Act statement provides the individual sufficient information to allow the individual to make an informed decision about whether to provide the requested PII. For example, Pursuant to OMB Circular A-108 and DoD 5400.11-R, the Privacy Act Statement must include:

- The authority that authorizes the collection of PII.
- The principal purpose or purposes for which the PII will be used.
- The routine uses that will be made of the PII.
- Whether providing the PII is voluntary or not.
- The effects on the individual if the individual does not provide the PII.
- An appropriate citation (and, if practicable, a link) to the relevant SORN(s).

The DHA Privacy Office helps to ensure that DHA follows the requirement for providing individuals with a Privacy Act Statement at the time of collecting PII for an SOR. For example, the DHA Privacy Office handles DHA Privacy Act related questions and reviews DHA systems to determine if they comply with the Privacy Act.

5.1.3 Computer Matching Agreements (CMA) Program

The Privacy Act and DoD 5400.11-R require that DHA obtains a CMA when automated data is matched between two or more automated SORs to determine eligibility for a federal

service or benefit. A CMA is a written and executed agreement between the source agency, or the agency providing the records for matching, and a recipient agency – a federal or non-federal agency that receives the records. In conformance with the Privacy Act, DoD 5400.11-R requires specific elements to be included in CMAs. DHA participates in a major matching program with HHS. DHA employees must not disclose any records contained in a SOR to a recipient agency for use in a computer matching program, except in compliance with a written agreement between DHA and the recipient agency, as well as an appropriate notice of this activity in the Federal Register.

DoD 5400.11-R also authorizes the Defense Data Integrity Board. The Defense Data Integrity Board oversees and coordinates all CMAs involving personal records contained in SORs maintained by the DoD components. This means that the board reviews and approves CMAs between the DoD and other federal, State, or local government agencies, as well as any memorandums of understanding, when the match is internal to the DoD. This review ensures that appropriate procedural and due process requirements are established before engaging in the CMAs. The members of the Defense Data Integrity Board include: representatives designated by the Secretaries of the Military Departments; the DoD CIO; the General Counsel of the DoD; the Inspector General of the DoD, who is a nonvoting advisory member; the Director, Enterprise Information Technology Services Directorate; and the Director, Defense Manpower Data Center.

5.1.4 SSN Use, Reduction, and Elimination Program

Due to the elevated risk of identity theft, DoD 5400.11-R provides requirements on the collection of SSNs and DoD regulation 32 Code of Federal Regulations (CFR) 157.1-157.8 establishes the DoD SSN Reduction Plan. The review of SSN use and justifications is included in the biennial Privacy Act SORNs review and should be included in the FISMA reporting requirements.

The DHA Privacy Office has developed a plan to review the use of SSNs and to reduce DHA reliance on SSNs, which reduces the risk to individuals of having their identity compromised if there is a privacy breach involving SSNs. The DHA Privacy Office works with SORs Managers and System Owners to reduce the volume of SSNs collected and retained to the minimum necessary to accomplish a business function, and to limit the number of employees who have access to SSNs to only those with a need to know in order to complete their job functions.

5.1.5 Privacy Considerations for Contracts and Interagency Agreements

Pursuant to the Privacy Act Section (m)(1), and DoD 5400.11-R C1.3, the DHA Office of Acquisitions and Assistance (OAA) must work with Program Managers, SOR Managers, and System Owners to include appropriate privacy protection language in contracts and interagency agreements. This language ensures that the government contractor or servicing agency complies with the Privacy Act and other federal authorities, including the E-Gov Act Section 208.

The Federal Acquisition Regulation (48 CFR) Part 24, Protection of Privacy and Freedom of Information and 52.239–1 Privacy or Security Safeguards, is the mechanism that requires OAA to insert certain language in contracts to ensure compliance with privacy requirements. DHA Privacy Office regularly reviews, updates as necessary, and approves the language to be included in DHA contracts to protect privacy. According to DHA Privacy Office guidance, some of the key privacy protections that should be considered in contracts, include:

- **a.** DHA control of PII in systems for the length of the contract and beyond;
- **b.** Contractor or service provider has no ownership of the PII;
- **c.** Contractor or service provider has no access or retention rights to the PII beyond those authorized by the contract and only during the life of the contract;
- **d.** Contractor or service provider must provide DHA access to PII when needed; and
- **e.** Contractor or service provider must comply with the contract responsibilities and are subject to liabilities for PII incidents and breach response activities.

The DHA Privacy Office website provides the specific contract language required at: https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language?type=Forms+%26+Templates.

5.2 E-GOVERNMENT ACT OF 2002 (SECTION 208 AND FISMA)

Section 208 of the E-Gov Act mandates privacy protection requirements for federal information systems and Title III of the E-Gov Act, FISMA, imposes security requirements for federal information systems. These protections may overlap and include: preparing PIAs, posting privacy notices on websites that comply with E-Gov requirements, ensuring that agency privacy policies are provided on the website in machine-readable format, providing information security related training, and reporting to OMB and Congress on privacy and security system compliance. OMB and NIST have both provided further guidance towards implementing these requirements, as discussed below.

5.2.1 Privacy Threshold Analysis

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* provides the original guidance that organizations should conduct a PTA as an initial privacy assessment to determine whether PII exists on a system, whether a PIA is needed as required by Section 208 of the E-Gov Act, whether a SORN is needed, and if any other privacy requirements are needed.

The DHA CPO uses the PTA or privacy risk assessment as the first step in determining the necessary privacy protections for an information collection. The DHA PTA or privacy risk assessment determines: (1) whether an activity involves PII or otherwise may impact privacy; (2) whether a PIA is required; and (3) whether an existing SORN covers an information collection, or if a new one is required. The privacy risk assessment is also the means by which DHA ensures that privacy is considered in systems undergoing assessment, and for assisting in determining the security categorization of a system based on the potential impact to the organization or individuals should there be a breach of security. The DHA CPO can work with the Program Manager or System Owner to complete the privacy risk assessment.

5.2.2 PIAs

Section 208 of the E-Gov Act of 2002 (Public Law 107-347, 44 United States Code (U.S.C.) Ch 36) requires agencies to conduct a PIA before initiating a new collection of information in identifiable form and before developing or procuring IT to collect, maintain, or disseminate PII. Section 208 also requires agencies to maintain privacy policies on their websites and requires policies to be translated into a machine-readable format.

In accordance with Section 208 requirements and OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, DHA System Owners conduct a PIA before developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or before initiating (consistent with the Paperwork Reduction Act of 1980, see 44 U.S.C. §§ 3501-3521), a new electronic collection of information in identifiable form for ten or more persons (excluding agencies, instrumentalities or employees of the federal government). In addition, pursuant to the guidelines in OMB M-10-23, *Guidance for Agency Use of Third Party Websites and Applications*, DHA conducts a PIA when DHA, or a DHA contractor on the Agency's behalf, uses a third-party website site or application to engage with the public.

The DHA Privacy Office PIA team coordinates the PIA process within DHA in compliance with the above stated authorities and guidance and in compliance with DoD policy

document DoDI 5400.16, DoD PIA Guidance. DHA Privacy Office PIA team ensures that PIAs are conducted using an approved PIA template. A PIA conducted by another federal agency does not fulfill DHA's PIA requirement, even when such an agency is providing computing services for DHA. The DHA Privacy Office PIA team assists DHA System Owners and developers who collect, maintain, and/or disseminate PII in demonstrating the incorporation of required privacy protections throughout the entire life cycle of a system. The DHA Privacy Office uses the PIA to:

- Determine the risks and effects of collecting, using, maintaining, and disseminating PII; and
- Evaluate protections and alternative processes for handling PII to mitigate potential privacy risks
- Ensure compliance with related provisions, in collaboration with other offices, such as the Records Office

The length and breadth of a PIA will vary by the size and complexity of the program or system, or the amount and types of PII involved. A System Owner must demonstrate through the PIA, for any new system that involves PII that they conducted an in-depth analysis to ensure that they have built privacy protections into the system. DHA must update PIAs to reflect changed information collection authorities, business processes, or other factors affecting the PII. In addition, DHA must conduct and update PIAs where a significant system change creates new privacy risks, or every 3 years.

5.2.3 Privacy Notice

The DHA CPO ensures that MHS provides notice to the public – through Privacy Act Statements, online and other public-facing privacy policies, PIAs, and SORNs – about how a program, system, or technology will impact their privacy. For example, the notice describes how PII will be used, shared, retained, disclosed, and destroyed. In general, notice is provided prior to and/or at the time of information collection or creation, unless otherwise directed by applicable laws, directives, policies, or regulations. Notice is intended to inform individuals about (1) what information is being collected; (2) the purpose of the collection; (3) how the information is used; (4) to whom the information is disclosed and shared; (5) individuals' rights under the Privacy Act to access and amend or correct their records to the extent practicable; and (6) the types of redress programs available. To the extent practicable, notice also states how long the information is retained and what the consequences are for failure to provide the information requested.

5.2.4 Inventory of Personally Identifiable Information

In support of the Privacy Act and FISMA, OMB issued M-07-16, *Safeguarding Against and Responding to a Breach of Personally Identifiable Information* which reiterates the

guidance in OMB Circular A-130, Appendix II, and provides that agencies must review PII holdings to make sure they are accurate, relevant, and timely. NIST SP 800-122 also provides this same guidance to agencies.

DHA reviews its PII holdings periodically and ensures to the maximum extent practicable that such holdings are accurate, relevant, timely, and complete, and reduces them to the minimum necessary for the proper performance of a documented DHA function. The DHA Privacy Office has created and updates periodically an inventory that contains a listing of all information systems, information collection forms, and SORs identified as involving the collection, use, maintenance, or dissemination of PII. The DHA Privacy Office uses this baseline PII inventory to evaluate DHA collection, use, maintenance, and dissemination of PII and to identify areas where DHA can reduce or eliminate its dependence on PII.

5.2.5 Annual Reporting on Compliance

FISMA requires agency compliance with standardized system security and privacy requirements, and requires an annual report that goes to OMB and Congress after the end of each fiscal year. This annual FISMA Report consists of gathering a large amount of information on system compliance from both a security and privacy perspective, and includes information on the completion of SORNs and PIAs, reduction of SSN use, and implementation of RMF controls, among other data elements, across the agency.

As provided below in section 9.0, the DHA CPO reports jointly with the DHA CIO in response to a set of questions that may vary each year, based on what OMB determines to be the priority activities for reporting. The DHA CPO provides the DHA CISO with Privacy Program metrics and related information required to meet the organization's FISMA privacy reporting requirements.

In addition to FISMA reporting, Section 803 Reporting is requirement twice a year for regular Federal Privacy and for Civil Liberties programs, chiefly focusing on whether complaints in those areas were received by the component, and if so, how they were resolved.

5.2.6 Training in IT Security and Privacy

FISMA requires training in security and privacy topics related to information systems and related fields based on roles. DHA meets this requirement by requiring workplace training in IT security awareness, HIPAA, and Privacy Act upon initial employment, and annually thereafter. DHA provides additional role-based training, such as HIPAA Privacy Officer and HIPAA Security Officer training, for those filling roles with privacy and security

responsibilities throughout the DHA. For more information on training, please refer to section 11.0, Privacy Training and Awareness.

5.3 PAPERWORK REDUCTION ACT (PRA)

The PRA and subsequent regulatory guidance established requirements for information collection requests (ICRs) and for minimizing the paperwork burden for individuals, small businesses, educational, nonprofit institutions, Federal contractors, state, local and tribal governments, and other persons from the collection of information by or for the Federal Government. Surveys, questionnaires, registration forms, websites, and databases are representative of the types of ICRs subject to the PRA requirements.

DHA Program Managers and System Owners must work with Office of Records Management to comply with the numerous OMB guidance documents for ICRs. Information collections are subject to all federal privacy compliance requirements, including PTAs, PIAs, Privacy Act Statements, and SORNs. DHA Program Managers, SORs Managers, Information System Owners, Information System Security Manager, and Information System Security Officers (ISSOs) must complete these privacy compliance documents before a DHA program starts to collect information related to the ICR and before they make any changes to the program's information collection process. The DHA Privacy Office coordinates with the Information Management Collection Officer regarding compliance with PRA in relation to privacy compliance documents.

6.0 HIPAA

6.1 GENERAL OVERVIEW

HIPAA was enacted by Congress in 1996 with the goal of improving the efficiency and effectiveness of the health care system. The HIPAA legislative statute includes five titles. The Administrative Simplification portion of HIPAA (Title II) mandated six interrelated standards – resulting in the HIPAA Privacy, Security, and Breach Notification Rules. The Administrative Simplification portion is found within Subtitle F of Title II. It requires that HHS adopt standards for the electronic transmission of certain health information.

The HIPAA Rules have been updated throughout the years to keep pace with evolving technology and the resulting privacy and security concerns. Most recently, in January 2013, HHS issued the Omnibus Final Rule which implements a number of provisions of the HITECH Act. These updates became effective in September 2013.

HIPAA regulates CEs, which include health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a standard transaction set forth in the regulations. HIPAA also regulates Business Associates (BAs), which are entities that provide a service to a CE and require PHI to perform the service. The MHS must comply with the requirements of the HIPAA Rules, both as a provider of health care – through MTFs – and as the TRICARE health plan – through contracted network health care services. To implement the HIPAA Rules, DoD issued privacy and security standards for safeguarding the confidentiality, integrity, and availability of PHI within all DoD components required to comply with the HIPAA Rules, as well as the permitted and required uses and disclosures of PHI by such components.

The HIPAA Privacy Rule establishes the minimum safeguards to protect the confidentiality of health information in all its forms – paper, electronic, and verbal. It also establishes standards for the handling, use, and disclosure of an individual's health information. The HIPAA Privacy Rule provides a minimum set of protections – or a federal floor – for individuals' privacy and establishes individual rights. It does not "take away" or reduce any privacy protections that are otherwise provided. The HIPAA Privacy Rule also establishes administrative requirements of CEs and BAs.

The HIPAA Security Rule establishes a federal floor of minimum standards to ensure the confidentiality, integrity, and availability, of electronic protected health information (ePHI). The HIPAA Security Rule establishes a national set of standards for protecting ePHI that is created, received, maintained, or transmitted in electronic form by a CE or a BA. In practice, the HIPAA Security Rule requires CEs and BAs to: ensure the CIA of all ePHI the CE or BA creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI; protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted by the HIPAA Privacy Rule; and ensure workforce compliance.

The HIPAA Breach Notification Rule requires HIPAA CEs and their BAs to provide notification following a breach of unsecured PHI. The HIPAA Breach Notification Rule defines breach as the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule and which compromises the security or privacy of the PHI. Upon discovery of a breach of unsecured PHI, a CE must notify each individual who may have been affected by the breach, as well as the HHS Secretary, and, in some cases, the media. BAs are required to notify the CE upon discovery of a breach.

6.2 DOD'S ORGANIZATIONAL STRUCTURE UNDER HIPAA

Unless otherwise structured, an organization regulated by HIPAA is deemed a single CE, and the entire organization must comply with HIPAA. This means that all components of the organization, including any components that do not engage in covered functions (also known as non-covered components) must be trained and adhere to all of HIPAA's privacy, security, breach notification, and enforcement standards for safeguarding PHI. CEs that are legally separate, but under common ownership and control, are able to designate themselves as a "single affiliated CE." In a single affiliated CE, all of the affiliated CEs function as one HIPAA CE, sharing the same HIPAA policies, procedures, and notice of privacy practices.

When an organization includes both covered and non-covered components, however, HIPAA provides an option for the organization to structure and declare itself a "hybrid entity." In a hybrid entity, only the organization's covered components and components acting as BAs of covered components are identified as "health care components" and required to comply with HIPAA. This enables the organization to implement HIPAA in a manner that reduces unnecessary exposure to administrative obligations, legal risks, and unintended costs. Due to a lack of clarity when HIPAA was enacted as to whether affiliated CEs could designate themselves as a hybrid entity, DoD declared its affiliated CEs within the MHS as a single CE. However, DoD functionally structured itself as a hybrid entity. The upcoming updates to DoD's HIPAA Privacy Rule implementation regulation provide further clarification by designating the DoD as a hybrid entity.

6.3 HIPAA COMPLIANCE WITHIN DOD

DHA must meet the objectives of the HIPAA Privacy and Security Rules to ensure that when PHI is collected, maintained, used, disclosed or transmitted that reasonable and appropriate administrative, physical. and technical safeguards have been implemented to ensure integrity, availability and confidentiality. Such measures are in the form of policies and procedures (administrative) as well as technical and physical safeguards and are intended to provide protection against any reasonably anticipated threats or hazards. These safeguards also ensure that the information is used and disclosed only as permitted by the HIPAA Privacy Rule, and ensure that the DHA workforce complies with the HIPAA training requirements. The requirements of the HIPAA Privacy and Security Rules as implemented within the DoD are extensive; however, the core tenets and activities are captured in the DHA HIPAA Privacy and Security Core Tenets Policy Statement, available on the DHA Privacy Office website, and include:

6.3.1 Designation of a HIPAA Privacy/Security Officer

The Director of the DHA Privacy Office is the DHA HIPAA Privacy and Security Officer and has the responsibility and authority for the development, implementation, maintenance, oversight, and reporting of privacy and security requirements for PHI. The HIPAA Privacy and Security Officer provides strategic and tactical program direction. The HIPAA Privacy and Security Officer is responsible for the development and implementation of the policies and procedures required by Federal legislation that pertain to the privacy and security of PHI, as well as the corresponding DoD Regulations.

6.3.2 Workforce Training

DHA must train its workforce on their roles and responsibilities for protecting PHI. As such, DHA has developed and implemented a HIPAA awareness and training program for all members of the workforce. The awareness portion of the program includes information papers on HIPAA privacy and security topics, brownbag lectures, list serves, eNews and weekly email reminders. The training component of the program consists of formal computer based courses delivered through JKO. Workforce training materials are reviewed and updated, as appropriate, on an annual basis.

6.3.3 Policy Development and Review

DHA must implement and maintain reasonable and appropriate policies and procedures that provide privacy and security protections for all PHI. These policies and procedures must include: (1) A purpose and scope that states expected goals; (2) Responsibilities; and (3) Criteria for meeting the requirements. Procedures must also include: (1) Clarification on where, how, when, about what and to whom, a procedure applies; (2) Clearly defined responsibilities and expected behaviors for the effected members of the workforce; and (3) Appropriate points of contact.

6.3.4 Use and Disclosure Notice

As required by the HIPAA Privacy Rule and DoD 6025.18-R, DHA provides individuals with a notice of uses and disclosures of PHI that may be made by the organization and informs them of their rights and DHA's legal duties with respect to PHI. This notice is provided by the MHS Notice of Privacy Practices and can be found on the DHA Privacy Office website.

6.3.5 Complaints

DHA has a process in place for individuals to file complaints concerning potential HIPAA violations which stem from an MHS MTF or covered entity.. The process ensures that DHA documents all complaints received and their disposition. In addition to HIPAA complaints directly submitted to DHA, complaints may also be submitted to HHS. When

this occurs, HHS Office of Civil Rights refers them to the DHA Privacy Office for investigation and final adjudication. The DHA Privacy Office coordinates with the appropriate Service associated with the respective MTF where the issue occurred, and prepares all correspondence to the complainant, the Services, and ultimately back to HHS in those applicable instances.

6.3.6 Sanctions

DHA must ensure that sanction policies are in place and applied appropriately against workforce members who fail to comply with the HIPAA privacy/security policies and procedures of the organization. DHA uses standard disciplinary processes, when appropriate, to determine specific sanctions according to the severity and circumstances of violations. This is done in collaboration with DHA's Human Resources staff.

6.3.7 Business Associate Agreements

BAs of DHA are authorized to create, use, receive, maintain, or transmit PHI on behalf of the organization provided that appropriate assurances are presented to the organization that the BA will appropriately use and safeguard the information on its behalf. DHA must ensure satisfactory assurances that meet these requirements are documented through a written contract or other legal arrangement with the BA. Under HITECH, BAs are directly accountable for their compliance with the HIPAA Security Rule and portions of the HIPAA Privacy Rule. The DHA Privacy Office, in collaboration with the Contracting Office Directorate, has developed standard BA clauses that address Privacy and HIPAA requirements.

6.3.8 Breach Response and Notification

Responsibility for breach notification expanded with the HITECH Act and the HIPAA Breach Notification Rule. A "breach," as defined by HHS differs from the broader definition established by DoD policy. The Chief of the DHA Privacy Office coordinates comprehensive breach response efforts, to include reporting, monitoring, and remediation efforts within the MHS. Breach response procedures for both PHI and PII breaches are discussed in Section 11.0.

6.3.9 Safeguards

Appropriate administrative, technical, and physical safeguards are necessary to protect the privacy and security of PHI at DHA. The safeguards must reasonably protect health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements and to limit incidental uses or disclosures, and the strength of the protection measures must be commensurate with the projected level of harm if a breach were to occur. The HIPAA Privacy and Security

Officer oversees the requirements for the administrative, technical, and physical safeguards required by HIPAA but the execution of the requirements are carried out by multiple offices within DHA.

6.3.10 HIPAA Privacy and Security Risk Management

The DHA Privacy Office conducts annual HIPAA Security Risk Assessments for safeguards found enumerated in DoDI 8580.02. During this assessment, each safeguard is evaluated for potential impact of perceived threats and their exploitation against vulnerabilities, and appropriate remediation actions are recommended. DHA Privacy Office also supports the review and development of over 200+ specific privacy related controls in the protection of PII and PHI for NSS in conformance to the CNSS Instruction No. 1253 Appendix F, Attachment 6 (Privacy Overlays). As part of the CRA, the DHA Privacy Office assesses the compliance posture of a random sample of DHA offices and their contractors to ensure ongoing adherence to these requirements.

The DHA Privacy Office reviews various documents and agreements to ensure that appropriate HIPAA Security safeguards and provisions are included. These agreements include System Security Verifications (SSV), PIAs, and Memorandum of Agreements (MOA); and Memorandum of Understanding (MOU).

- SSVs are a part of the DHA Data Sharing Agreement process. They are required whenever a data requestor seeks to use or maintain PHI on an information system that has not been granted an authority to operate (ATO) by the DoD. SSVs provide a description of the security posture of the data requestor's organization, with specific emphasis on the HIPAA Security safeguards found in DoDI 8580.02
- As part of the PIA review and approval internal process, the DHA Privacy Office reviews DHA PIAs to see appropriate HIPAA Security safeguards are included
- MOAs/MOUs are reviewed to make sure that appropriate HIPAA Security references and requirements are incorporated into these agreements

6.3.11 Individual Rights

The HIPAA Privacy Rule and DoD 6025.18-R provides the following rights to individuals:

(1) Right to inspect and copy PHI in a designated record set;
(2) Right to request amendment to PHI in a designated record set;
(3) Right to receive a notice of privacy practices that includes how health information may be used and shared;
(4) Right to request restrictions of PHI that is used or disclosed for certain purposes;
(5) Right to receive confidential communications by alternative means or at alternative locations;
(6) Right to request an accounting of certain disclosures of PHI; and

(7) Right to file a complaint with DHA and/or with the Office for Civil Rights.

These rights are limited by the scope of the regulations, as have been and will continue to be explained in HIPAA training and in related DoD issuances. DHA has documented procedures in place to adhere to these individual rights.

7.0 Data Sharing

Both the Privacy Act and HIPAA Privacy Rule require that certain privacy and security protections be met before sharing PII or PHI and that specific privacy language be included in data sharing agreements, depending on the data shared and the purpose for which it is shared. In addition, OMB and NIST guidance outlines best privacy practices and provides specific security and privacy controls that must be met in sharing data through contracts.

The DHA Privacy Office receives various types of research requests for DHA data. Under its Data Sharing Program, the DHA Privacy Office reviews each request for compliance with applicable federal law and implementing DoD policies.

7.1 DATA SHARING AGREEMENT APPLICATIONS

The DHA Privacy Office provides a DSAA for the applicants and Government Sponsors (requestors) to complete when requesting DHA data. The DSAA requires the requestors to provide the purpose for the request as well as specify the data elements required. The DHA Privacy Office uses the information provided in the DSAA to confirm the type of data requested: de-identified data, limited data set (LDS), PII that does not include PHI, and PHI. Once the type of data requests is determined, the DHA Privacy Office can conduct all necessary compliance reviews and ensure that the requested data will be safeguarded in compliance with applicable Federal laws and DoD policies. The DHA Privacy Office incorporates the DSAA into the final executed DSA. By signing the DSA the Government Sponsor and applicant acknowledge their role in maintaining their compliance and ensuring the safety of DHA managed data.

7.2 DATA EVALUATION WORKGROUP (DEW)

The DEW includes members of the DHA Privacy Office Data Sharing team, the HRPP team, the DHA Privacy Board staff, and data experts. The DEW meets weekly to review and discuss the progress of DSAAs. The DEW mission is to determine the type of data request based on the information provided in the DSAA. In addition to determining the type of data requested, the DEW discusses the best sources for the requested data and the minimum necessary amount of data a researcher will need. During the DEW, the members

discuss their progress in talking to requestors about the purpose of their studies, the data elements requested, and how the requestors can minimize the data elements. Once the DEW determines the type of data being requested, the DHA Privacy Office completes the compliance review process and ensures the correct DSA is executed. If the data determination is PHI, the DEW sends the request to the DHA Privacy Board for a HIPAA compliance review.

7.3 DHA HIPAA PRIVACY BOARD

As required by HIPAA, the DHA Privacy Office established a DHA Privacy Board to provide HIPAA Privacy Rule reviews and documentation for researchers that seek to use and/or disclose PHI managed by DHA. The DHA Privacy Board is critical for DHA's compliance with the HIPAA Privacy Rule (45 CFR 160 & 164) and DoD Health Information Privacy Regulation (DoD 6025.18-R). As required by the HIPAA Privacy Rule and DoD Health Information Privacy Regulation (DoD 6025.18-R), the DHA Privacy Board:

- Consists of HRPP Program Managers of varying and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
- Includes at least one member who is not affiliated with the HIPAA CE (DHA within the MHS), not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
- Does not have any member participating in a review of any project in which the member has a conflict of interest.

The DHA Privacy Board reviews Institutional Review Board (IRB) approved documentation of full or partial waivers of authorization and altered authorizations. The board also provides templates for researchers to complete in requesting data for several different types of research projects. These templates help researchers to obtain approved compliance documentation from the board for the following:

- HIPAA Authorizations
- Altered Authorization
- Full or Partial Waivers of Authorization
- Required Representations for Review on Decedents' Information only; and
- Required Representations for Review Preparatory to Research

Once the DHA Privacy Board approves the compliance documentation submitted by the researchers, the board notifies the DHA Privacy Office Data Sharing team that HIPAA compliance has been met.

In addition to board reviews and maintaining HIPAA compliance documentation of DHA PHI requests, the DHA Privacy Board meets quarterly to discuss the board metrics and current related topics. DHA Privacy Board staff also assists researchers and the research community by responding to questions related to HIPAA compliance requirements.

7.4 SSV REVIEWS

Occasionally data requestors will seek to use, store, transmit, process or otherwise maintain DHA PHI or LDS data obtained through the DSA process on an information system that has not been granted a DoD ATO or Interim Approval To Operate. In those instances, the requestors are required to complete an SSV. The SSV is a template, designed by the DHA Privacy Office, to address the requirements of DoDI 8580.02 and the safeguards outlined in DoDI 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems. A member of the DHA Privacy Office Security team reviews each SSV to determine if the privacy and security posture of an organization is conclusive in nature. The SSV is considered part of the DSAA approval process and an approved SSV is incorporated into an executed DSA.

7.5 DSA

After all compliance reviews are completed, the DHA Privacy Office Data Sharing Compliance team completes the execution of the DSA. Depending on the type of data requested and the required assurances for compliance standards, the requestors will sign one of four template DSAs:

- De-identified data DSA;
- PII that is not PHI DSA;
- LDS; or
- PHI DSA.

The DSAs incorporate the DSAA into the agreement as further evidence of the data elements requested and the compliance requirements that the requestors must meet in receiving DHA data.

8.0 FOIA

FOIA is a federal law enacted in 1966 that grants the public access to information possessed by government agencies after any exempt material has been removed (redacted). Upon request, United States Government agencies are required to release information unless it falls under one of the nine exemptions. All executive branch departments, agencies, and offices are subject to FOIA. However, it does not apply to Congress, federal courts, and parts of the Executive Office of the President that serve only to advise and assist the President. FOIA is enforceable in a court of law.

8.1 FOIA DISCLOSURE LIMITATIONS

FOIA provides that any person has a right, enforceable in court, to obtain access to federal agency records, except such records (or portions of them) that FOIA exempts from public disclosure. Under FOIA, agencies must disclose any requested records, except such records (or portions of them) that FOIA exempts protected from public disclosure. The FOIA exemptions provide protection for nine categories of records, including records, the disclosure of which, would constitute a clearly unwarranted invasion of personal privacy. The DHA Privacy Office collaborates closely with OGC regarding FOIA exemptions in reviewing documents for release.

9.0 Civil Liberties

Civil liberties are personal rights and freedoms that are either explicitly guaranteed by the Constitution and specifically the Bill of Rights, or by interpretation by courts and legislators. Examples include: freedom of speech, freedom of religion, freedom to bear arms, and freedom to be free of unreasonable searches and seizures, as well as a right to privacy, right to travel, etc. Agencies having substantial homeland security information, such as DoD, are mandated by statute to establish Civil Liberties programs to ensure that the rights of citizens are protected in this era of necessary information sharing. The DHA Privacy Office ensures such compliance through policies and procedures, complaints processing, training and awareness, reporting requirements, and consultation with related offices. The DHA is committed to protecting the civil liberties of its workforce (civilian employees, uniformed Service members, and contractors), customers (active duty, Veterans and family members), and members of the public.

In 2007, the Defense Privacy and Civil Liberties Office (DPCLO) directed that every DoD organization implement and administer an official Civil Liberties Program as mandated by

Section 803, Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007 ("9/11 Commission Act"). Accordingly, the DoD established, what is now the DHA Privacy Office to establish the Civil Liberties program within the DHA. The DHA Privacy Office Chief was designated by the DHA Director as the DHA Civil Liberties Officer.

The DHA Privacy Office is charged to protect the personal freedoms of DHA workforce members, their beneficiaries, and of those individuals with whom they interact. The Administrative Instruction No. 64 (AI-064) establishes policy and assigns responsibilities for the implementation of the DHA Civil Liberties Program. The AI-064 integrates requirements from the DPCLO for best practice Civil Liberties component programs. Primary responsibilities of a component Civil Liberties Program include: education and outreach to DHA workforce members; policy and procedure development; adjudication and resolution of civil liberties complaints; fulfilling reporting requirements to DoD, and ultimately Congress; promoting a climate of civil liberties awareness and compliance; and participating as a Board Member in the greater DoD Civil Liberties Board. The DHA Civil Liberties Program has won awards for its Outstanding Program in 2013, 2014, and 2015 and was designated the Top Program for 2014 and 2015 among DoD components. The model program evaluation process was discontinued by the DPCLTD in 2016 because substantial progress was achieved by component civil liberties programs across DoD.

10.0 Breach Prevention and Response

10.1 BREACH RESPONSE

Enclosure 3, Procedures, of DHA-AI 071, Incident Response Team (IRT) and Breach Response Requirements, provides the procedures for the DHA workforce to use to help prevent, detect, and respond to any potential or confirmed breaches of PII or PHI. The Appendices at the end of DHA-AI 071 also provide tables, checklists, and templates to use in responding to a breach, including:

- DHA Reporting/Notification Guidelines Table
- DHA Breach Response Checklist
- Guidelines for Reporting Breaches
- DHA Breach Risk Analysis Template
- Plan of Action and Milestone Template
- After Action Report Template
- Communication Templates
- Sample Notification Letter Template

- Congressional Information Paper/Letter Template
- Sample Substitute Notice Template
- Sample Media Announcement Template

Enclosure 2, Responsibilities, of DHA-AI 071 identifies members of the IRT. In addition to the IRT Co-Chairs (DHA Chief of Staff (CoS) and the DHA CPO), members of the IRT include the: DHA Privacy Office; OGC; Office of the Director, DHA (Front Office); DHA Communications Division; Administration and Management Division; Business Support Directorate; Relevant Program Office; and HIT Directorate, for electronic breaches.

Enclosure 2, Responsibilities, of DHA-AI 071 clearly delineates the responsibilities of all IRT members in regard to:

- Reporting suspected or confirmed incidents involving PII;
- Convening the breach response team to determine the appropriate course of action in the event of a privacy incident; and
- Notifying National Cybersecurity and Communications Integration Center (NCCIC) and, as necessary, affected individuals, appropriate organization staff offices, the Inspector General, Congress, law enforcement, and the press.

10.2 PRIVACY INCIDENT RESPONSE PLAN

Planning and preparing for privacy incidents requires development of reporting and notification procedures for all levels of responders: senior leadership; managers of programs experiencing a breach; CPO; CIO; CISO; legal counsel; Office of the Inspector General; Communications Office; Legislative Affairs Office; the Management Office (including budget and procurement functions); and the information security incident center (help desk). An effective privacy incident response plan also requires educating all employees and contractors on when and how to report privacy incidents.

The DHA Privacy Office coordinates breach reporting within the MHS, for both breaches involving PII and for breaches involving PHI. DoDD 5400.11, DoD Privacy Program, defines breach, as follows:

> "A 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."

The DHA Privacy Office will determine whether a breach meets the requirements of reporting to the HHS.

10.3 TRACKING PRIVACY INCIDENTS

Enclosure 2, Responsibilities, of DHA-AI 071 assigns responsibility for maintaining all documentation related to a breach to the IRT Co-Chairs, which consist of the DHA CoS and the CPO. The CPO is responsible for maintaining comprehensive files on each suspected or confirmed breach detailing actions taken, to include executive summaries, e-mail communication, letters, breach response status reports, and meeting minutes for documentation, historical, and lessons learned purposes. DHA-AI 071 further assigns responsibility for addressing each stage of incident handling. The reporting tiers have been restricted to the minimum necessary, while ensuring that officials responsible for safeguarding PII are fully informed regarding incidents.

10.4 CONTINGENCY PLANNING

Currently, the DHA Privacy and Civil Liberties Office coordinates its contingency planning and practices with DHA senior leadership as evidenced through the IRT and Breach Response Requirements in accordance with Administrative Instruction (AI) 071. Additionally, specific planning as it relates to the information type PII and PHI are coordinated with DHA HIT as necessary.

DHA-AI 071 outlines the breach response processes and procedures established to identify, mitigate, and contain the potential damage from the loss/compromise of PII and PHI data and institutes a standard process and procedure for reporting and responding to breaches. The Director, DHA, is responsible for the implementation of DHA-AI 071 to safeguard the privacy and security of PII/PHI entrusted to the DHA and to ensure reasonable and appropriate safeguards are maintained for all such PII/PHI created, maintained, received, or transmitted through electronic or non-electronic media.

Enclosure 2, Responsibilities, of DHA-AI 071 identifies members of the IRT and assigns roles and responsibilities to each. The IRT Co-Chairs have lead responsibility for coordinating investigations and responses. This involves coordinating with the Business Support Directorate and other necessary Directorates and staff in estimating the costs of a breach including, but not limited to: notifying potentially affected individuals who experience issues with their credit, offering credit monitoring, providing restoration services for affected individuals, the establishment of a call center, mailings, etc. The Comptroller is responsible for assessing the financial implications of the breach and determining costs associated with impact, risk, and mitigation for the breach, and must

propose an allocation of required resources and funding to the appropriate approval authority.

10.5 MANAGING PRIVACY COMPLAINTS AND REDRESS

The Privacy Act requires 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 Privacy Office has a process to review and adjudicate privacy complaints or inquiries. The procedures ensure that all complaints are recorded, tracked, and addressed. DHA also addresses, where applicable, procedures for coordinating redress among the entities that control the information in question or who are the nexus of the complaint.

11.0 Privacy and Cybersecurity Information Life Cycle Management

OMB Circular A-130 requires agencies to plan in an integrated manner for managing information throughout its life cycle. Information life cycle management requires robust privacy and security programs for the protection of PII and PHI collected, used, shared, retained, disclosed, and destroyed by the organization. Privacy and security programs are dependent on each other and have complementary objectives. For this reason, the DHA CPO and DHA CISO work together in a close partnership to ensure the success of both the privacy and cybersecurity program in meeting the requirements of federal privacy laws, regulations, and guidance, including: the Privacy Act, E-Gov Act, Paperwork Reduction Act, and HIPAA.

11.1 ROLE OF PRIVACY IN INFORMATION LIFE CYCLE MANAGEMENT

Based on the OMB and NIST guidance for implementing the federal privacy laws, the DHA Privacy Office works with DHA Cybersecurity to incorporate privacy analyses and controls into each stage of the information life cycle (i.e., collection, use, retention, processing, disclosure, and destruction) by doing the following:

- The DHA CPO keeps the DHA CISO informed of current statutory and regulatory privacy requirements for PII and PHI
- The DHA CPO works closely with the DHA CISO, program owners, and information system developers, as necessary, to identify systems containing PII and to ensure that appropriate protections are implemented and monitored. In this way, the DHA CPO can provide non-technical support to the CISO in implementing security controls to protect systems that contain PII

- Although privacy laws, regulations, and OMB and NIST guidance set minimum requirements for protecting PII, some categories of PII may require additional protections, based upon their sensitivity. When appropriate, the DHA CPO may determine and provide guidance that, for purposes of privacy risk mitigation, certain personal information maintained by an organization that is not expressly covered by privacy statutes or regulation may still require equivalent security controls
- The DHA CPO reviews systems and applications for privacy compliance and assesses the impact of the technology on privacy
- Currently the DHA Privacy Office conducts quarterly reviews of DHA information systems in the DoD Information Technology Portfolio Repository (DITPR) to ensure compliance with the privacy requirements of the E-Government Act and the Privacy Act. This includes validating PIAs and ensuring the correct SORNs are completed. Reviews of information systems in DITPR are conducted on an ongoing basis and each information system is reviewed at least once a quarter
- Organizations report annually on specific privacy and security activities in their annual FISMA reports to OMB. The DHA CPO reports jointly with the CIO in response to a set of questions that may vary each year, based on what OMB determines to be the priority activities for reporting. The DHA CPO provides the DHA CISO with Privacy Program metrics and related information required to meet the organization's FISMA privacy reporting requirements

11.2 ROLE OF SECURITY IN INFORMATION LIFE CYCLE MANAGEMENT

FISMA requires organizations to develop, document, and implement organization-wide programs to provide robust security for their information and information systems. The CPO plays a key role, in conjunction with the CIO, CISO, and other officials having privacy related responsibilities, as appropriate, in identifying risks to PII and taking steps to mitigate those risks using both privacy and security controls.

In that light, DHA incorporates privacy compliance requirements into its Assessment and Authorization (A&A) process, which is an evaluation of an IT system's risk and risk mitigation controls. The A&A process considers specific security requirements, verifies the existence of security controls, and summarizes residual risk. System Owners and ISSOs, in coordination with the DHA A&A implement the catalog of security and privacy controls in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. These controls provide a range of safeguards and

countermeasures for DHA information and information systems to protect against the loss, unauthorized access, or unauthorized disclosure of PII.

Using FIPPs, the NIST has developed guidance regarding privacy controls in NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J: Privacy Controls. The Privacy Controls provide a comprehensive framework for implementing privacy policy by providing a structured set of privacy controls based on best practices that will help DHA and the Privacy Program comply with federal privacy authorities. The Appendix J Privacy Controls establish a relationship between privacy and security controls for the purposes of enforcing privacy and security requirements within the NIST RMF. The DHA Privacy Office works in conjunction with Cybersecurity Services Division Assessment and Authorization Branch to interpret and implement the Appendix J Controls for DHA. Included in these implementation activities are responsibilities regarding the authorization to operate for information systems. Appendix J Privacy Controls ensure that specific requirements are met by systems undergoing the ATO process.

Table 3: Privacy Control Implementation

Privacy Control	DHA Implementation
Authority and Purpose (AP): This control family ensures that DHA identifies the legal bases that authorizes a particular PII collection or activity; and specifies in its notices the purposes for which PII is collected.	DHA uses the PII Inventory, PTA, PIA, Privacy Act Statement (also known as Privacy Act Notice), and SORN processes to identify the legal basis that authorize PII collection or activity that impacts privacy. DHA then uses PTAs, PIAs, Privacy Act Statements, and SORNs to provide notice of the purposes for which PII is collected.
Accountability, Audit, and Risk Management (AR): The AR control family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that DHA is complying with applicable privacy protection requirements and minimizing overall privacy risk.	DHA is accountable for compliance with all applicable privacy protection requirements, including all legal authorities and established policies and procedures that protect privacy and govern the collection, use, dissemination, and maintenance of PII. This also includes auditing for the use of PII to demonstrate compliance with established privacy controls. Accountability through effective monitoring and measurement controls builds public trust by demonstrating that an organization is complying with all of its applicable privacy protection requirements.
Data Quality and Integrity (DI): This control family enhances public confidence that any PII collected and maintained by DHA is accurate, relevant, timely, and complete for the	DHA takes steps to protect the quality and integrity of the PII that it collects, uses, maintains, and disseminates. All employees are responsible for using PII properly. This includes maintaining the quality and integrity of PII collected, used, maintained, and disseminated by DHA. DHA SOR Managers exercise due care in

purpose for which it is to be used, as specified in public notices.	ensuring that records containing PII are accurate, complete, timely, and relevant for Agency purposes. This is necessary to assure fairness in any determination about an individual. DHA SOR Managers implement security and privacy controls to maintain the accuracy and consistency of PII throughout the information life cycle. This is necessary to assure fairness in any determination about an individual.
Data Minimization and Retention (DM): This control family helps DHA to implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. DHA retains PII for only as long as necessary to fulfill the purposes specified in public notices and in accordance with a NARA-approved record retention schedule.	DHA collects, uses, and retains only PII that is relevant and necessary for the purpose for which it was originally collected, and retain PII only if necessary to fulfill the purposes specified in public notices and in accordance with a NARA-approved record retention schedule. All employees must use PII properly, and seek to reduce their use of PII and the volume and types of PII they collect. Employees must also retain PII only if necessary to accomplish their program purposes. DoDI 5015.02 reissues DoDD 5015.2 (Reference (a)) as a DoDI in accordance with the authority in DoDD 5144.02 (Reference (b)) to establish policy and assign responsibilities for the management of DoD records in all media, including electronic, in accordance with subchapter B, chapter XII, of Title 36, CFR and chapters 29, 31, 33, and 35 of Title 44, U.S.C. (References (c) and (d)).
Individual Participation and Redress (IP): The IP control family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in DHA decisions made based on the PII	This section addresses the policy requirements for Individual Participation and Redress. Participation includes consent and access to PII by the subject individual, and redress includes amendment of the PII and disseminating PII corrections to external partners with whom DHA shares the PII. The DHA Freedom of Information Service Center has principal authority to ensure HA, DHA, and its components are in full compliance with the FOIA. The Office of Management Services, is responsible for managing and responding to FOIA requests and Privacy Act access and amendment requests. The Office of Management Services is also responsible for managing correction dissemination and disclosure accounting functions, per the Privacy Act and 22 CFR 215, Regulations for Implementation of Privacy Act of 1974. The DHA Privacy Office manages FOIA requests directed to the DHA.
Security (SE): This control family supplements the security controls to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by DHA against loss, unauthorized	DHA addresses the policy requirements for Security functions specific to PII. The Privacy Program applies security controls to protect PII. Such security controls include identifying and reducing the use of PII and planning for, and responding to, privacy incidents.

access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST RMF.	
Transparency (TR): This control family ensures that DHA provides public notice of its information practices and the privacy impact of its programs and activities.	DHA provides public notice of its information practices and the privacy impact of its programs and activities. DHA accomplishes this function by posting Privacy Act Statements or Notices on DHA websites and paper forms and surveys, as well as posting website privacy policies, PTAs, PIAs, and SORNs on DHA public websites. Per the Privacy Act Section (e)(3), DHA must provide notice to individuals about whom it collects PII regarding: 1) The authority that authorizes the PII collection and whether disclosure by the individual of such PII is mandatory or voluntary; 2) The principal purposes for which the PII will be used; 3) The routine uses that may be made of PII; and 4) The effects on the individual of not providing all or any part of the requested information. As required, DHA ensures that the notices are located and accessible on the form or survey where the PII is collected, whether on a website, electronic media, or paper. A Privacy Act Statement or Notice is included on all DHA forms and surveys (both internal and external) that collect PII on individuals (citizens of the United States or aliens lawfully admitted for permanent residence).
Use Limitation (UL): This control family ensures that DHA only uses PII either as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.	This section addresses the policy requirements for SORNs under the Privacy Act. DHA must conform to the notice requirements of the Privacy Act of 1974. DHA must only use PII as specified in their public notices and in a manner compatible with those specified purposes, or as otherwise permitted by law. Employees must follow the Rules of Behavior for Users regarding the protection of PII or suffer the penalties enumerated in the Privacy Act and/or disciplinary actions. In addition, DHA shares PII only as authorized by law or for the authorized purposes in the Privacy Act and routine uses published in the appropriate SORN or Privacy Act Statement or Notice.

11.3 PRIVACY AND SECURITY CONTROLS WORKING TO PROTECT PII AND PHI IN NEW OR EMERGING TECHNOLOGY

As information and devices become increasingly mobile, and the amount of PII collected increases, it is more important than ever to consider privacy protections throughout the entire life cycle of existing and emerging technologies as part of DHA's PPP and as part of DHA's organizational risk management strategy. To protect PII and PHI in emerging technologies, DHA uses both automated privacy controls and privacy guidance and monitoring as follows:

12.3.1 Encryption as an Automated Privacy Control

Under various OMB memoranda and NIST security controls guidance, System Owners and ISSOs must ensure that all PII is encrypted at rest, in motion, during remote and wireless access, and on all removable media, such as laptops and Personal Digital Assistants (Blackberries and iPhones). Employees must ensure that PII is encrypted on all removable media, such as CDs and DVDs. Employees must also remove all PII from email strings and encrypt all PII in email attachments sent from DHA approved domains.

12.3.2 Cloud Computing

Cloud computing is internet-based computing whereby DHA contracts for shared resources, software, and information for computers and other devices. While this provides a flexible solution for complex IT needs, cloud computing poses additional privacy challenges for contract services. How a cloud services provider addresses privacy concerns within their environment may affect the overall price and technical structure for a proposed cloud computing solution. As a result, it is DHA's intent to gather privacy requirements as early as possible in the information life cycle to understand fully how to ensure that a cloud services provider maintains its duty to protect PII.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP provides Standard Contract Language that includes some appropriate privacy requirements for cloud computing contracts.

12.3.3 Data-Loss-Prevention (DLP)

DHA has implemented an automated DLP tool that is able to discover, monitor, and protect PII wherever it is stored or used across DHA systems. The DLP tool monitors how PII is used and where it goes in order to protect PII by automatically enforcing data loss policies;

educating users about data security; securing exposed data; and stopping data leaks. DHA currently uses the DLP tool to continuously monitor the DHA-managed email network to detect and prevent the movement of PII out of DHA-controlled networks.

The DHA Privacy Office routinely reviews the development of DHA policies and procedures that incorporates the use of DLP tools and similar technologies in an effort to monitor and reduce incidences of unauthorized disclosure of PII outside the DHA enclave. Currently, the DHA Privacy Office provides guidance and recommendations based on the data procured by these tools and other methods for breach incident response review determinations.

12.0 Privacy Training and Awareness

The HIPAA and Privacy Act training is required for all DHA civilian, military, and contractor personnel. The DHA Privacy Office is responsible for the development and availability of a merged course that offers specialized training unique to the MHS. These efforts are enhanced by promoting a culture of compliance through awareness, education, and outreach activities, including orientation sessions, annual seminars, routine newsletters and publications, and in-person training events.

Privacy training and awareness programs are key elements of building a culture of privacy throughout an organization. Training programs test and reinforce the implementation of privacy policy, providing a critical element of an effective Privacy Program. The CPO ensures that federal employees and contractors receive mandated privacy training. Through participant feedback, training and awareness programs provide valuable insight to help refine and improve privacy management and reduce the risk of privacy incidents throughout the organization. DHA provides annual privacy awareness training to all DHA employees and contractors. In addition, DHA provides targeted, role-based training to those employees and contractors designated as PII custodians, who will use or view PII data elements in the routine performance of their jobs.

12.1 MANDATORY TRAINING

The HIPAA and Privacy Act Training is a merged course which provides an overview of two critical privacy laws – HIPAA and the Privacy Act of 1974 – and discusses how these laws are applicable to the MHS. This training provides high-level regulatory standards that apply the same to operations staff, clinical staff, and senior management. It is divided into five modules followed by end-of-module exams that leads to a certificate of

completion. Module 1 provides a general overview of HIPAA, then explores the HIPAA Privacy Rule and correlating DoD Privacy Standards in greater detail. Module 2 focuses on the HIPAA Security Rule as well as DoD's implementation standards. Module 3 provides information about HIPAA Enforcement and HIPAA complaints. Module 4 focuses on the Privacy Act and the DoD Privacy Act Program. And, the final module, Module 5, covers Breach Response at DoD.

The HIPAA and Privacy Act Training is implemented on the eLearning enterprise platform, JKO. This training has an initial component and an annual refresher component that is triggered by the user's anniversary date on JKO. At the outset, users are prompted to indicate their roles within their organizations in order to access the training specific to their defined responsibilities. Each new user added to the DHA network is required to sign a form that includes an item about the timely completion of the HIPAA and Privacy Act Training within 30 days or the account will be disabled if this is not accomplished. Mandatory privacy training is provided at the New Hire Orientation and participants are provided with an information brochure on account creation and detailed instructions on accessing the HIPAA and Privacy Act Training on JKO.

Remedial training is also available where Training Managers can assign training out of cycle, should the need arise and as determined by the user's leadership. Record of completion will be maintained on the Administrative section of JKO and is readily available to the user and/or the Training Manager.

122 ROLE-BASED TRAINING

The HIPAA and Privacy Act Training provides high-level regulatory standards that apply the same to operations staff, clinical staff, and senior management. Throughout the training, users are directed to check with their respective senior management regarding more detailed role-based training for nuances based on specific roles as well as policies and procedures in different DoD healthcare entities that are not addressed in the training.

Advanced training is provided through the HIPAA Privacy and Security Officer Training on JKO, for designated HIPAA Privacy Officers, HIPAA Security Officers, and personnel with concurrent responsibilities. This training focuses on the portions of the HIPAA Rules that establish standards for the privacy and security of PHI – specifically the HIPAA Privacy and Security Rules. Additionally, an advanced training specific to Institutional Review Boards (IRBs) and HIPAA Privacy Boards was developed and implemented on JKO in November 2017. Entitled HIPAA Privacy Rule Compliance Training for IRBs and HIPAA Privacy Boards, this training will allow all IRBs, HIPAA Privacy Boards, and

offices overseeing human research protections to understand how to perform compliant HIPAA Privacy Rule reviews and how to use the HIPAA standard templates that are required for use in the electronic protocol management system. The online training will enhance HIPAA compliance across the MHS for research studies.

Additional privacy and/or security training is provided via onsite training that is also made available to remote participants, namely; the annual IRT Tabletop Exercise and the annual Health Information Privacy and Security (HIPS) Training. The IRT Tabletop Exercise enhances DHA preparedness and mitigation planning by exploring and addressing issues and implications concerning a simulated breach of PII and PHI affecting a large number of beneficiaries. The annual HIPS Training is held to supplement existing training available on JKO and other online platforms. This training provides a forum for interaction between subject matter experts and participants on pertinent privacy and security regulations. It integrates several interactive strategies to enhance learning and includes a Service Talk discussion which serves to highlight the privacy and security experiences of Service representatives from the Army, Air Force, Coast Guard and Navy. To coincide with each year's theme, a "Training Manual" is developed for distribution to participants as a product of the training and awareness program and contains a summary of key programs and initiatives that will help the reader in the complex and demanding HIPAA Privacy and Security world.

The DHA Privacy Office has a comprehensive program for job-specific and general privacy training for the DHA workforce (and the MHS with respect to the HIPAA Privacy, Security, and Breach Notification Rules) which are listed in Table 3 below.

Table 4: DHA Privacy Office Trainings

DHA Privacy Office Training	Description
DHA HIPAA, Privacy Act, and Civil Liberties Training	Annual initial and refresher training for all DHA workforce members as mandated by the Privacy Act, HIPAA, and Civil Liberties requirements. The course includes interactive features, incorporates HHS updates to the HIPAA Privacy, Security and Breach Notification Rules, and is made available to all MHS workforce members to enhance privacy compliance. This course was migrated to JKO from the MHS Learn Platform.
HIPS Training	The annual two-day HIPS Training serves as a forum to share best practices and expand upon important concepts related to privacy and security and the protection of PII and PHI. The training integrates several creative and interactive strategies used to enhance learning for

	both in-person and remote participants. These include animations, Service Talks discussion that include representatives from all four Services, a group-based learning workshop, a web-based learning game, collaborative pre- and post-tests, knowledge checks, and a robust tabletop exercise applying key concepts learned throughout HIPS Training.
DHA IRT Tabletop Exercise	The DHA IRT Tabletop Exercise features the Privacy Office's breach prevention efforts, which has resulted in a decrease in total breaches despite the Agency's continual growth and an overview of the seven steps to effective breach response.
HIPAA Privacy and Security Officer Training Course	The course focuses on the HIPAA Privacy, Security and Breach Notification Rules, as well as on HIPAA Compliance best practices. This course was implemented in February 2016 on JKO from TRICARE University and is available to over 500 HIPAA Privacy and HIPAA Security Officers within the MHS so they would be adequately informed of the role they play in protecting PHI.
HIPAA Privacy Rule Compliance Training for IRBs and HIPAA Privacy Boards	This course was developed as part of the DHA Privacy Office's Research Data Sharing Streamlining Initiative, and trains IRBs and HRPP on how to conduct data determinations leading to appropriate HIPAA reviews and how to conduct HIPAA Privacy Rule reviews of research studies.
DHA New Hire EoD Orientation Program	The DHA Privacy Office provides a briefing on the role of the DHA Privacy Office, required HIPAA, Privacy, and Information Assurance (IA) Training for new hires, and the core functions and responsibilities of the DHA Privacy Office.
Contractor Trainings	The CPO provides annual and bi-annual Managed Care Support Contractors, Designated Providers and Purchased Care contractors training programs which includes instruction on the core fundamentals of basic and electronic records management, the Privacy Act, PII and PHI, the TRICARE Operations Manual, DHA Records Freeze/Preservation Orders, Temporary Records Information Portal, breach prevention and reporting and electronic records storage initiatives, legal and practical issues involved in responding to FOIA requests, changes in federal civil rules, restrictions for disclosure of PHI mandated by HIPAA, and electronic records storage initiatives.
DHA Records Management Training	The "Striving for Teamwork in Action Records Seminar (STARS)" provided Records Management training and Privacy-specific sessions on the Federal DHA Data Sharing Process and Breach Prevention and Reporting.
Supervisory Training	On a quarterly basis, Supervisory Training is provided to Supervisors who are new, or receiving a three year refresher. During this two day event, the DHA Privacy Office provides a training segment targeted to special issues for supervisors.
Office Specific Training	Any office can request of the DHA Privacy Office a training event tailored to their needs. This occurs on a frequent basis.

Topical Trainings	When the DHA Privacy Office determines special topics warrant extra coverage, they may create a training event or a workshop to raise the level of knowledge. Recent examples include a workshop on Civil Liberties in the workplace, and on Privacy and SORNs.

12.3 TRAINING DELIVERY SYSTEM

The HIPAA and Privacy Act Training is available for access on JKO by members of the MHS workforce. The access to the Learning Management System (LMS) is Common Access Card -based and authenticated by a user Personal Identification Number when prompted by the system. Training records for all courses reside in the LMS and are readily accessible by the user for their own records and on an organizational level, by designated Training Managers. Compliance reports can be obtained to determine completions and/or discrepancies for each office, division, or organization, as structured in a domain tree that reflects the organizational hierarchy of the Services within the MHS.

13.0 Reporting Requirements

FISMA requires each federal agency to develop, document, and implement an agency-wide information security program. DoD reports quarterly and annually to OMB on progress in conducting PIAs and issuing SORNs for IT systems that are required to go through FISMA C&A. OMB requires organizations to use an automated system for submitting reports, thereby, enabling OMB to track, monitor, and report to Congress and the public on the progress made by individual organizations in their management of privacy. The DHA Privacy Office contributes to the DoD's quarterly and annual FISMA reports, including statistics on required and completed PIAs and SORNs for systems that are operational or that are registered in the organization's FISMA inventory system.

13.1 BREACH REPORTING

DHA must protect the information it collects, uses, maintains, and disseminates in support of its mission and business functions. Any unauthorized use, disclosure, or loss of such information can result in the loss of the public's trust and confidence in DHA's ability to safeguard information. PII/PHI breaches may have far-reaching implications for individuals whose PII is compromised, including identity theft resulting in financial loss and/or personal hardship experienced by the individual. Therefore, incidents involving a breach of PII/PHI have a critical time-period for reporting. As noted in Section 10, DHA-AI 071, Defense Health Agency Incident Response Team and Breach Response Requirements, establishes the processes and procedures for individuals and supervisors

responsible for assessing and responding to a confirmed or suspected breach of PII and/or PHI that occurs within the DHA.

13.2 SECTION 803 REPORTING

The CPO reports to OMB on a quarterly and annual basis per the requirements of the FISMA and Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1 (2012) (Section 803. The DHA CPO, reports statistics as requested by DPCLTD, which may include statistics on outstanding and completed PIAs and SORNs for DHA systems and MHS systems as applicable, as well as other data requested by OMB, or the number and outcome of any Privacy Act or Civil Liberties complaints. When DHA conducts a PIA or creates a SORN, it must report it to OMB under FISMA. The CSOP may also need to respond to congressional inquiries on an ad hoc basis.

13.3 INTERNAL REPORTING

Internal reporting may take several forms, such as data calls, weekly or monthly reporting to senior management on Privacy Program activities. MHS requires sub-organization or component program progress and compliance reporting to their individual leadership as well as to the CPO. The DHA Privacy Office reviews incident reporting data at least quarterly to assess both enterprise and component compliance.

14.0 Privacy Consultation

In its responsibilities for day-to-day activities, the DHA Privacy Office supports other programs and participates in working groups and privacy and security briefings. The DHA Privacy Office encourages requests for consultation early in any process in which privacy issues may surface, and is strongly in favor of supporting the mission of program offices with workable and helpful solutions.

14.1 WORKING GROUPS

To ensure that both Privacy Act and HIPAA requirements are addressed for DHA and MHS systems and operations, the CPO oversees the DHA Privacy Office's participation in a wide range of DoD and DHA working groups and committees, included but not limited to:

- Cybersecurity Working Group and Defense Health Clinical Systems Working Group meetings to assess DHA systems and ensure privacy has been appropriately considered and addressed

- The CNSS' Privacy Overlay Tiger Team in the development of the Privacy Overlay, establishing over 200 specific privacy and security controls designed to protect PII and PHI. The DHA Privacy Office provides HIPAA subject matter expert supports for the Privacy Overlay Tiger Team
- The Functional Advisory Council that oversees development of business requirements for initial operating capability and final operating capability business process models for the DoD electronic health record (EHR) and the Health Information Exchange (HIE) Working Group that defines HIE functional requirements. Participation in these groups helps to enable HIE and EHR compliance with the HIPAA Privacy and Security Rules and related DoD policies

DHA Privacy Office also regularly participates in various meetings for HIE, Health Records Working Group, Mobile Technology Working Group, RMF WG, Protected Health Information Management Tool (PHIMT), Precision Care Advisory Panel, the DHA Privacy Board, and other groups wherever privacy subject matter expertise is sought.

14.2 INFORMATION DISSEMINATION

The CPO keeps the MHS community abreast of emerging legislative and policy efforts via the Health Information Privacy and Security Compliance Committee. The CPO also ensures relevant legislative and regulatory guidance from the OMB, HHS, DoD and DHA are posted on the DHA Privacy Office website.

The DHA external website, health.mil, and DHA internal SharePoint site, LaunchPad are used to disseminate awareness and guidance documents, including DHA HIPAA privacy and security information papers and tips of the day for protecting PHI. The DHA Privacy Office also publishes monthly Privacy Post newsletters which are distributed throughout the DHA and feature articles on HIPAA, the Privacy Act, Civil Liberties, and information security topics.

15.0 Conclusion

The DHA Privacy Office is tasked with safeguarding the privacy and security of PII and PHI. The DHA Privacy Office supports MHS' mission and business functions by assisting in balancing the need to maintain and in many cases share information about individuals while protecting the information against unwarranted invasions of individual's privacy

resulting from the collection, maintenance, use, and dissemination of this personal information.

This document is meant to be used as a resource by offices and individuals within the DHA. It will be updated periodically by the DHA Privacy Office to reflect changes in the DoD environment and guidance provided by various DoD and regulatory authorities. The plan will be refined as needed to anticipate impacts to DHA's privacy posture and to identify the best responses for emerging issues.

APPENDIX A: ACRONYMS

A&A	Assessment and Authorization
AI	Administrative Instruction
AP	Authority and Purpose
AR	Accountability, Audit and Risk Management
ATO	Authority to Operate
BA	Business Associate
CFR	Code of Federal Regulations
CoS	Chief of Staff
CNSS	Committee on National Security Systems
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Computer Matching Agreements
CPO	Chief Privacy Officer
CSOP	Component Senior Officials for Privacy
CSIRT	Computer Security Incident Response Team
DHA	Defense Health Agency
DI	Data Quality and Integrity
DITPR	DoD Information Technology Portfolio Repository
DLP	Data Loss Prevention
DoD	Department of Defense
DoDD	DoD Directive
DODI	DoD Instruction
DPCLTD	Defense Privacy, Civil Liberties and Transparency Division
DPCLO	Defense Privacy and Civil Liberties Office
DSA	Data Sharing Agreement
DSAA	Data Sharing Agreement Application
DEW	Data Evaluation Workgroup
ePHI	Electronic Protected Health Information
EHR	Electronic Health Record
FedRAMP	Federal Risk and Authorization Management Program
FCWG	Functional Capability Work Group
FIPP	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
HA	Health Affairs
HHS	Health and Human Services
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act

HIPS	Health Information Privacy and Security
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health
ICR	Information Collection Request
IP	Individual Participation and Redress
IRB	Institutional Review Board
IRT	Incident Response Team
ISSO	Information System Security Officer
IT	Information Technology
JKO	Joint Knowledge Online
LDS	Limited Data Set
LMS	Learning Management System
MHS	Military Health System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTF	Military Treatment Facility
MTWG	Mobile Technology Working Group
NARA	National Archives and Records Administration
NDAA	National Defense Authorization Act
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NSS	National Security Systems
OAA	Office of Acquisitions and Assistance
OASD[HA]	Office of the Assistant Secretary of Defense for Health Affairs
OGC	Office of the General Counsel
OMB	Office of Management and Budget
PCM	Privacy Continuous Monitoring
PHI	Protected Health Information
PHIMT	Protected Health Information Management Tool
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PPP	Privacy Program Plan
PRA	Paperwork Reduction Act
PTA	Privacy Threshold Analysis
RMF	Risk Management Framework
SAOP	Senior Agency Official for Privacy
SOR	System of Record
SORN	System of Records Notice
SP	Special Publication
SSN	Social Security Number
SSV	System Security Verification

STARS	Striving for Teamwork in Action Records Seminar
TMA	TRICARE Management Activity
U.S.C.	Unites States Code

APPENDIX B: STATUTES AND REGULATIONS

Laws and Regulations:

- Federal Information Security Management Act of 2002, Title III – Information Security, P.L. 107-347
- Federal Information Security Management Act of 2014, P.L. 113-283
- E-Government Act of 2002, Section 208
- 22 CFR 215
- Administrative Procedure Act of 1946
- Federal Acquisition Regulation (FAR) (48 CFR) Part 24, Protection of Privacy and Freedom of Information
- The FAR (48 CFR) 52.239–1 Privacy or Security Safeguards
- Health Information Portability and Accountability Act of 1996
- Paperwork Reduction Act of 1995
- Privacy Act of 1974

OMB Circulars:

- OMB Circular A-130, *Management of Federal Information Resources*, November 2000.
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information

FIPS Publications:

- FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006

NIST Publications:

- NIST 800-18 Revision 1, *Guide for Developing Security Plans for Information Technology Systems*, February 2006
- NIST 800-30, *Risk Management Guide for Information Technology Systems*, July 2002
- NIST 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010
- NIST 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010
- NIST 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002

- NIST 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013
- NIST 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010
- NIST 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security*, August 2008
- NIST 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012
- NIST 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, April 2006
- NIST 800-64 Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004
- NIST 800-122, *Guide for Protecting the Confidentiality of Personally Identifiable Information*, April 2010
- NIST 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011

APPENDIX C: DEFINITIONS

The terms and definitions listed below have been incorporated into the DHA PPP. These terms and their definitions are for purposes of this DHA PPP.

access
The ability or the means necessary to read, write, modify, or communicate data or information, or otherwise use any system resource.

breach
The 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 personally identifiable information, whether physical or electronic.

cloud computing
Internet-based computing whereby shared resources, software, and information are provided to computers and other devices.

contractor
This term refers to independent contractors and institutional contractors.

disclosure
Dissemination or communication of any information that has been retrieved from a protected record by any means of communication (written, oral, electronic, or mechanical) without written request by or consent of the individual to whom the record pertains.

dissemination of information
Actively distributing information to the public at the initiative of the agency.

employees
Includes DHA direct-hire personnel, fellows, interns, contractors, and any other category of person, not a contractor, requiring a security clearance to work on DHA information or material or have unescorted access in DHA space.

encryption
This is the act of transforming information into an unintelligible form, specifically to obscure its meaning or content.

individual

A citizen of the United States or an alien lawfully admitted for permanent residence.

information life cycle
The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

information system
The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. This term includes both automated and manual information systems.

Information System Security Officer
Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

maintain
Collection, use, updating, sharing, disclosure, dissemination, transfer, and storage of personally identifiable information.

matching agreement
The agreement establishing the terms of a matching program between DHA and another federal or non-federal agency.

matching program
A computerized comparison of two or more automated system of records (SOR), or a SOR with non-federal records.

personally identifiable information
Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Same as "information in an identifiable form" and records about individuals in a "system of records".

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

Privacy Act Notice
A statement or notice, required by Privacy Act Section (e)(3), appearing on a Web site or information collection form notifies the users of the authority for collecting requested information. It also states the purpose and use of the collected information. DHA must notify the public or users if providing such information is voluntary or mandatory, and the effects, if any, of not providing all or any portion of the requested information. See also Privacy Act Statement.

Privacy Act Statement
A statement or notice, required by Privacy Act Section (e)(3), appearing on a Web site or information collection form notifies the users of the authority for collecting requested information. It also states the purpose and use of the collected information. The public or users must be notified if providing such information is voluntary or mandatory, and the effects, if any, of not providing all or any portion of the requested information. See also Privacy Act Notice.

Privacy Impact Assessment
Analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in electronic information systems; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

privacy incident
A violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of PII, whether in electronic or paper format.

Privacy Threshold Analysis
Analysis of whether a program or system has privacy implications, and if additional privacy compliance documentation is required, such as a Privacy Impact Assessment or System of Records Notice.

system
Refers to any information system or application, and may be used to designate both the hardware and software that comprise it.

system of records
A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of Records Manager
Individual responsible for daily program and operational management of their specific DHA Privacy Act System of Records. System of Records Managers are responsible for ensuring that their System of Records and the related DHA program comply with the requirements of the Privacy Act.

System of Records Notice
A notice of the existence and character of the system of records, which notice shall include— (1) the name and location of the system; (2) the categories of individuals on whom records are maintained in the system; (3) the categories of records maintained in the system; (4) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (5) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (6) the title and business address of the agency official who is responsible for the system of records; (7) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; (8) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and (9) the categories of sources of records in the system.

System Owner
Individual responsible for daily program and operational management of their specific DHA system. System Owners are responsible for ensuring that a security plan is prepared, implementing the plan and monitoring its effectiveness.

unauthorized disclosure
when PII is disclosed to anyone except the subject individual absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory conditions in the Privacy Act, 5 USC 552a(b)(1) -(12).

use
The sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information.

APPENDIX D: TABLE OF REQUIREMENTS

Privacy Program Compliance Requirements

Compliance	Requirements	Summary
Privacy Act	Account of Certain Disclosures	The disclosure of Privacy Act-protected PII outside of normal processing and allowed exception should be recorded and maintained for five years after the disclosure. (§552a.(c))
Privacy Act	Access/Amendment Request for PII	Access and amendment request for Privacy Act-protected PII, the disposition of those requests, and the time consumed to process them should be maintained to validate that requirements are being followed. (§552a.(d))
Privacy Act	Contest Findings of Computer Matching Program	All records pertaining to an individual's complaints about a matching program's findings and subsequent processing should be maintained to validate the requirements are followed. (§552a.(d))
Privacy Act	Explicit Consents	The Privacy Act requires written consent for certain disclosures of PII; the written consents should be maintained. (§552a.(b))
Privacy Act, E-Government Act	Privacy Training	Each person involved in the design, development, operation, and maintenance should be instructed on the privacy rules of behavior; and training records should be kept. (§552a.(e)(9))
Privacy Act, FISMA	Computer Matching Program Records	PII records processed by a computer matching program must be maintained and be accessible to other organizations (for example, GAO) for auditing or investigatory purposes.
Privacy Act, FISMA	SORN Status and SORNS	Each PP store should be evaluated to determine if a SORN is needed. Either a SORN or documented justification for a SORN's absence should exist. Such as justification must identify who authorized the decision and include specific exemptions.
Privacy Act, FISMA, OMB-07-16	Privacy Violations Including Privacy Breaches	Instances of agency Privacy Act violations and the details surrounding the violations must be recorded and maintained.
E-Government Act, FISMA	Machine-Readable Web Privacy Policy Status	A record should be maintained for each of the agency's public websites on its status

		relative to having a machine-readable policy.
E-Government Act, FISMA	Persistent Tracking Use	Records need to be maintained about where tracking technology is used, why it is needed, controls used to protect the tracked information, how the public is notified of tracking and the agency official who approved tracking.
E-Government Act, FISMA	PII Status and PIAs	Each electronic PII store should be evaluated to determine if a PIA is needed. Either a PIA or documented justification for a PIA's absence should exist. Such a justification must identify who authorized the decision.
FISMA	PII Store(s) Inventory	An inventory of applicable electronic systems and hard copy records (such as paper copies) must be recorded and maintained.
OMB Circular A-130, Appendix I	Privacy Act Mandated Review	A record should be kept of the annual and two-, three- and four-year reviews mandated by OMB Circular A-130.
Freedom of Information Act (FOIA)	FOIA Requests and Results	A record of all FOIA requests, appeals, denials, and processing time and fees must be kept.
OMB M-07-16	Signed Acknowledgement of Responsibilities for Protecting Privacy and Security of Information	Agencies must ensure that individuals who are authorized access to PII and their supervisors sign a document at least annually that clearly describes their responsibilities for protecting the privacy and security of that information.

APPENDIX E: CNSS 1253 PRIVACY CONTROLS MAPPING

Control Number	CCI	CCI Definition	PPP Section
AR-1	CCI-003401	The organization monitors federal privacy laws and policy for changes that affect the privacy program.	1.2: Authority
AR-1	CCI-003402	The organization defines the allocation of budget resources sufficient to implement and operate the organization-wide privacy program.	3.0: Privacy Program Primary Roles and Responsibilities
AR-1	CCI-003403	The organization defines the allocation of staffing resources sufficient to implement and operate the organization-wide privacy program.	3.0: Privacy Program Primary Roles and Responsibilities
AR-1	CCI-003404	The organization allocates sufficient organization-defined budget resources to implement and operate the organization-wide privacy program.	3.0: Privacy Program Primary Roles and Responsibilities
AR-1	CCI-003405	The organization allocates sufficient organization-defined staffing resources to implement and operate the organization-wide privacy program.	3.0: Privacy Program Primary Roles and Responsibilities
AR-1	CCI-003406	The organization develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures.	5.0: Federal Agency Privacy Compliance
AR-2	CCI-003417	The organization documents a privacy risk management process which assesses the privacy risk to individuals.	12.3: Privacy and Security Controls working to Protect PII and PHI in new or emerging technology
AR-2	CCI-003425	The organization conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.	5.2.2: Privacy Impact Assessment
AR-4	CCI-003434	The organization defines the frequency for monitoring privacy controls and internal privacy policy to ensure effective implementation.	Table 2: Privacy Control Implementation

AR-4	CCI-003439	The organization audits internal privacy policy, per organization-defined frequency, to ensure effective implementation.	Table 2: Privacy Control Implementation
AR-5	CCI-003440	The organization develops a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.	13.0: Privacy Training and Awareness
AR-5	CCI-003443	The organization defines the frequency, minimally annually, for administering its basic privacy training.	13.0: Privacy Training and Awareness
AR-5	CCI-003444	The organization defines the frequency, minimally annually, for administering the targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII.	13.0: Privacy Training and Awareness
DI-1	CCI-003470	The organization issues guidelines ensuring the quality of disseminated Privacy Act information.	5.1: Privacy Act of 1974
DI-2	CCI-003483	The organization's Data Integrity Board oversees the organizational Computer Matching Agreements.	5.1.3: Computer Matching Agreement
DI-2	CCI-003484	The organization's Data Integrity Board ensures the Computer Matching Agreements comply with the computer matching provisions of the Privacy Act.	5.1.3: Computer Matching Agreement
DI-2(1)	CCI-003485	The organization publishes Computer Matching Agreements on its public website.	5.1.3: Computer Matching Agreement
DM-1	CCI-003491	The organization establishes a schedule for regularly reviewing the PII holdings on an organization-defined frequency to ensure that only PII identified in the notice is collected and retained.	5.2.4: Inventory of PII
DM-1	CCI-003492	The organization follows a schedule for regularly reviewing the PII holdings on an organization-defined frequency to ensure that only PII identified in the notice is collected and retained.	5.2.4: Inventory of PII

Document Review History

The PPP is reviewed, at a minimum, semi-annually, and review history is tracked in the table below.

Version	Review Date	Comments/Notes	Reviewed By	Signature
Version 1.0	Feb 2, 2018	Minor grammatical updates; added text to Section 11.4, 12.3.3, and 13.2	DHA Privacy Office	
Version 1.4	Sep 19, 2018	Minor grammatical updates; revision to section 3.0, 5.1, 5.2, 7.1, and 7.3	DHA Privacy Office	
Version 1.6	Mar 27, 2019	Minor grammatical updates; revision to section 6.3.5, 10.1, 10.4, removed section on Human Research Protection Program	DHA Privacy Office	