



HEALTH INFORMATION PRIVACY & SECURITY

TRAINING MANUAL

JUNE 2015



DHA PRIVACY & CIVIL LIBERTIES OFFICE





**DHA PRIVACY AND
CIVIL LIBERTIES OFFICE**

Defending Privacy

7700 Arlington Blvd
Suite 5101
Falls Church, VA 22042
703-681-7500

WELCOME LETTER

DHA Privacy and Civil Liberties Office

Greetings from the Defense Health Agency (DHA) Privacy and Civil Liberties Office (Privacy Office),

The vision of the DHA is to serve as a joint, integrated, premier system of health, supporting those who serve in the defense of our country. Every day we continue to strengthen our efforts and capabilities toward this vital mission. Our resolve is strong in support of this mission!

The DHA Privacy Office fully supports this endeavor by ensuring vigilance in the protection of information privacy, promoting related compliance across the organization, and enhancing value by ensuring peace of mind as well as public trust. As DHA continues to develop towards Full Operating Capability, we also assume our role by establishing alliances with stakeholders in the shared service vision. Our work cannot succeed without the strong collaboration among all parties in this new environment. We are grateful for the firm commitment we see across the board to the privacy protection and compliance principles we uphold.

The DHA Privacy Office's essential mission is unchanged: fostering and maintaining compliance with the Privacy Act, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security, and Civil Liberties regulations; processing Freedom of Information Act requests; and managing our Data Sharing and Human Research Protection Programs.

Each member of the DHA workforce and the Military Health System contributes to the privacy protection mission through your day-to-day adherence to our HIPAA and Privacy Act information protection standards. As a result, we are in a strong position for protecting privacy information, and you deserve thanks and significant credit. It is a thriving endeavor in large part because of you!

It is my hope that this booklet will assist you with useful guidance and tools to support your privacy-related activities at the DHA. Also, remember that the DHA Privacy Office is always available to assist you with any questions or concerns you may have.

With best wishes and thanks,

Chief, DHA Privacy and Civil Liberties Office



TABLE OF CONTENTS

Introduction.....	4
HIPAA Privacy	7
HIPAA Security	13
Privacy Overlays.....	18
HIPAA Transactions, Code Sets, and Identifiers.....	21
Data Sharing	23
Human Research Protection Program	27
Breach Response.....	29
External Compliance Oversight.....	35
Military Command Exception	37
Emerging Technology	42
Federal Privacy Requirements	46
DHA’s Civil Liberties Program	53
Freedom of Information Act.....	56

INTRODUCTION

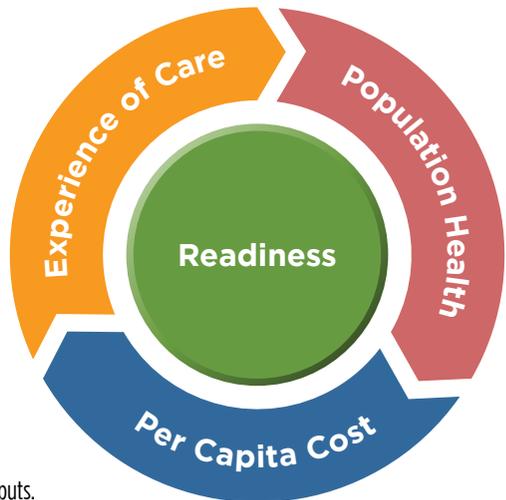
Defense Health Agency

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 and ready medical force to Combatant Commands in both peacetime and wartime. Established October 2013, its mission is to be: “A joint, integrated, premier system of health, supporting those who serve in the defense of our country.” This includes achieving greater streamlining of our healthcare delivery systems through the use of shared services and by other means so that we accomplish the Military Health System’s (MHS) Quadruple Aim: achieve medical readiness, improve the health of our people, enhance the experience of care, and lower our healthcare costs. The DHA, since its startup in 2013, is transitioning towards full operational capability as of October 1, 2015.

The DHA supports the delivery of integrated, affordable, and high quality health services to MHS beneficiaries and thereby, supports the Quadruple Aim.

THE QUADRUPLE AIM

-  Enabling a medically ready force, a ready medical force, and resiliency of all MHS personnel.
-  Improving quality and health outcomes for a defined population. Advocating and incentivizing health behaviors.
-  Patient and family centered care that is seamless and integrated. Providing patients the care they need, exactly when and where they need it.
-  Managing the cost of providing care for the population. Eliminate waste and reduce unwarranted variation; reward outcomes, not outputs.



DHA PRIVACY AND CIVIL LIBERTIES OFFICE

The DHA Privacy and Civil Liberties Office (Privacy Office), under the direction of DHA's Administration and Management Directorate, oversees the protection of personally identifiable information (PII) and protected health information (PHI) within the MHS, one of the largest integrated healthcare delivery systems in the United States, serving over 9.6 million eligible beneficiaries. The DHA Privacy Office supports MHS compliance with federal privacy and HIPAA laws, and DoD regulations and guidelines. Each core program within the DHA Privacy Office facilitates this mission by:

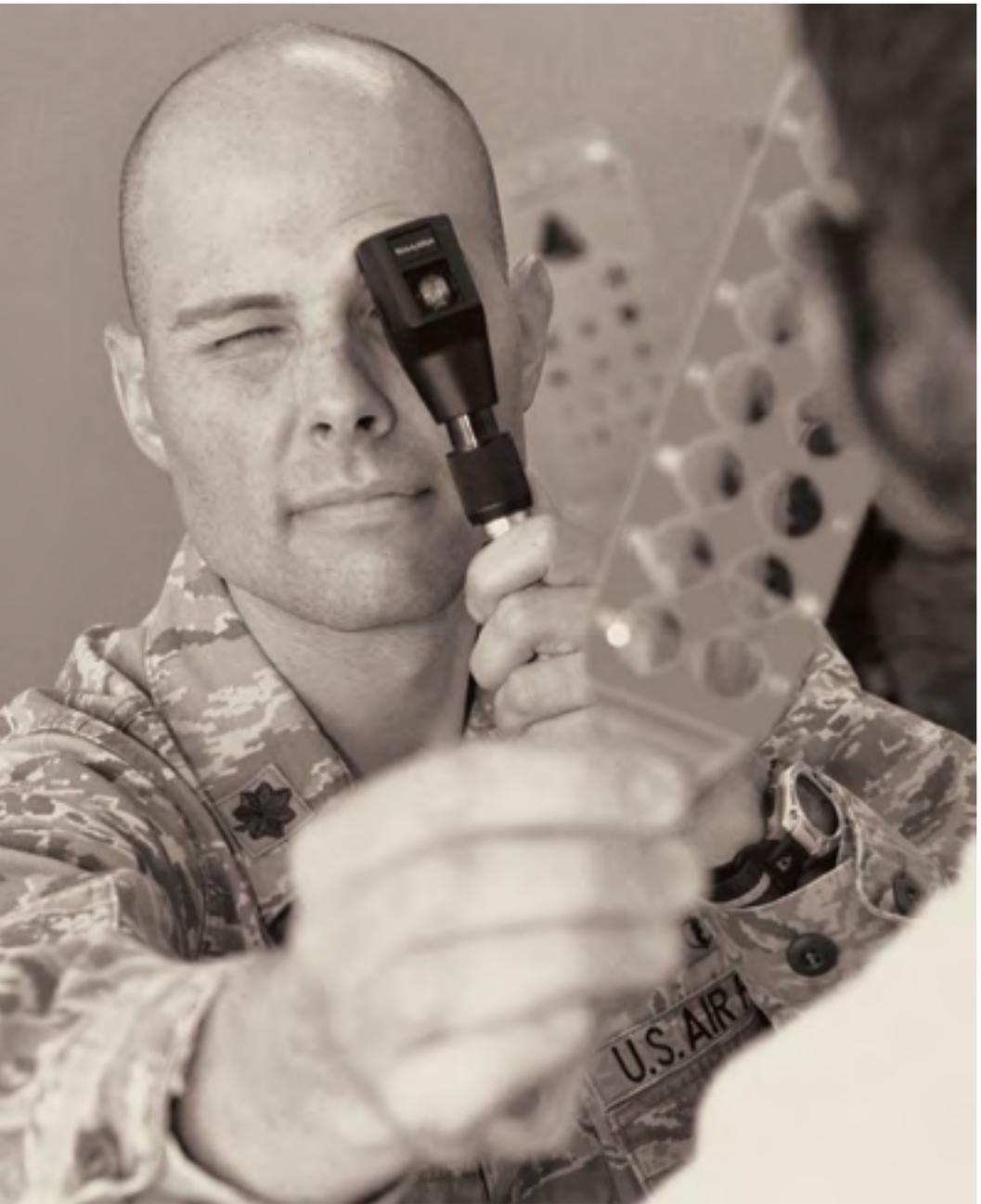
- Providing guidance and oversight for Privacy and HIPAA matters
- Assessing risk and responding to HIPAA complaints or breach incidents
- Developing and delivering training and awareness materials to the workforce
- Managing related programs, including Civil Liberties, Freedom of Information Act, Data Sharing, and Human Research Protection
- Providing consultation and assistance to leadership and the workforce on internal and external matters
- Providing privacy expertise in workgroups for several ventures, including electronic health records

HEALTH INFORMATION PRIVACY AND SECURITY TRAINING MANUAL

This training manual is a product of our training and awareness program, and contains a summary of key programs, initiatives, and tools that will help the reader navigate the complex and demanding world of privacy and HIPAA. Contained in the



program overviews are references to more detailed information for each subject, along with relevant resources and contact information. The back pocket of the manual contains a CD with the presentations from the June 9-10, 2015 Health Information Privacy and Security Training given annually by the DHA Privacy Office.



HIPAA PRIVACY

Complying with the HIPAA Privacy Rule within the Military Health System

Safeguarding the privacy and security of health information is a major concern. The HIPAA Privacy Rule, originally issued in 2003 and updated in 2013, was issued by the Department of Health and Human Services (HHS), in part, to address this concern. The MHS must comply with the requirements of the HIPAA Privacy Rule, both as a provider of health care through Military Treatment Facilities (MTFs) and as the TRICARE health plan. The HIPAA Privacy Rule focuses on permitted uses and disclosures of protected health information (PHI) as well as individual rights with respect to PHI created or received by covered entities (CEs), including the MHS.

The HIPAA Privacy Rule was implemented within DoD through DoD 6025.18-R, the DoD Health Information Privacy Regulation, dated January 24, 2003. This document is currently under revision and will be reissued as a DoD Instruction in the near future.

KEY TERMS

Business Associate (BA) – A person or entity who is not a member of the CE’s workforce that creates, receives, maintains, or transmits PHI on behalf of the CE or in providing a service to the CE that involves the use or disclosure of PHI. DoD CE BA’s may include other DoD CEs, other DoD components, other federal agencies, contractors supporting DoD CEs, and others. See DoD 6025.18-R, paragraph C3.4.1.

Business Associate Agreement (BAA) – A legal agreement between a CE and its BA that outlines responsibilities and obligations for compliance with the HIPAA Rules and the handling of PHI. Requirements for DoD CE BAAs are set forth in

DoD 6025.18-R, paragraphs C3.4.2 and C3.4.3. Approved BAA language and formats for use by DoD CEs is available at <http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language>.

Covered Entity (CE) – A health plan, healthcare clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a HIPAA transaction. CEs within DoD are generally defined or identified in DoD 6025.18-R, paragraph C3.3.

Disclosure – The release, transfer, provision of access to, or revealing in any other manner of PHI outside the entity holding the information. A

“disclosure of PHI” by a DoD CE occurs even if the PHI is provided to another DoD component, not just when PHI is provided to a person, agency, or entity outside the DoD.

Health Insurance Portability and Accountability Act (HIPAA) – Law that directed the establishment of comprehensive and uniform federal standards for the protection of health information. It applies to CEs, which are: healthcare plans, healthcare clearinghouses, and certain healthcare providers. The law is implemented by the HHS through the adoption of standards, including standards for protecting the privacy and security of individually identifiable health information, which are commonly referred to as the HIPAA Privacy Rule and the HIPAA Security Rule.

Minimum Necessary – Limiting the use, disclosure, and request for PHI to only the minimum amount needed to carry out the use or purpose of the disclosure. Exceptions to this standard are as follows:

- Disclosures to or requests by a healthcare provider (without regard to whether the requesting provider is a CE) for treatment purposes
- Disclosures to individuals or pursuant to individual’s authorization
- Disclosures to HHS for HIPAA compliance purposes
- Uses or disclosures required by law

Notice of Privacy Practices (NoPP) – Document generated by a CE that describes how an individual’s PHI may be used/disclosed, outlines individual privacy rights, describes CE obligations

under the HIPAA Privacy Rule, and outlines the process for filing a complaint.

Organized Health Care Arrangement (OHCA) – The MHS and certain elements of the U.S. Coast Guard are, under DoD 6025.18-R, considered to be an OHCA. This status allows members of the OHCA to also exchange PHI with each other for treatment, payment, and healthcare operations (TPO) purposes, have a joint NoPP, and share a common BA.

Protected Health Information (PHI) – Individually identifiable health information that relates to the individual’s past, present, or future physical or mental health, the provision of health care, or the payment for health services, and that identifies the individual or it is reasonable to believe the information can be used to identify the individual. PHI excludes information contained in employment records held by a CE in its role as an employer. Because DoD is a federal agency, PHI of a DoD CE is also “personally identifiable information” under the Privacy Act of 1974.

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

PATIENT RIGHTS UNDER THE HIPAA PRIVACY RULE

HIPAA requires individuals be given certain rights, and the CE is responsible for responding to an individual’s request to invoke any of these rights. In applying these rights within the MHS in connection with a minor, add the ability of parent, guardian, or person acting in loco parentis of a minor, the MHS applies the State law of where the treatment is provided. See DoD 6025.18-R, paragraphs C2.4.2.1 and C8.7.3.

These rights are listed below:

RIGHT TO A NoPP

Individuals have a right to be notified how their PHI may be used and/or disclosed by the CE. Individuals must also be notified of their rights and the CE's legal responsibilities with respect to their PHI. See DoD 6025.18-R, Chapter 9.

RIGHT TO INSPECT AND COPY

Individuals have a right to inspect and request a copy of their PHI held by a DoD CE in a designated record (including an electronic copy, if maintained electronically). A CE must respond within 30 days after the receipt of a request, but with written explanation, may obtain an additional 30 days and must provide a date certain for production. Under certain circumstances, a CE may deny such requests, in whole or in part, but must provide a written explanation of the denial, and in some cases, an opportunity to have the denial reviewed. DoD 6025.18-R, Chapter 10, provides information on the process and procedures to be followed by an individual in submitting a request to inspect or copy, and by a DoD CE receiving such a request.

RIGHT TO FILE A COMPLAINT

Individuals have the right to file a complaint directly with an MTF HIPAA Privacy Office, the DHA Privacy Office, and/or the HHS Office for Civil Rights if they feel a CE has committed a violation of the HIPAA Privacy or Security Rule provisions. A CE must provide a process for individuals to make complaints concerning the CE's policies and procedures under the HIPAA Privacy Rule. DoD 6025.18-R, paragraph 14.4, provides information on the process and procedures to be followed by an individual in submitting a complaint and by a DoD CE receiving a complaint.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

Individuals have a right to request their PHI be communicated in a certain way or at a certain location (e.g., only at home or only by mail). A CE must accommodate reasonable requests. DoD 6025.18-R, paragraph 10.2, provides information on the types of requests that may be made, how a request is to be filed, and the actions to be taken by a DoD CE in connection with approving or denying such requests.

RIGHT TO REQUEST RESTRICTIONS

Individuals have a right to request a CE restrict the use or disclosure of their PHI for TPO purposes or to persons involved in the individual's care or healthcare payment. A CE is not required to agree to a restriction request except in certain circumstances, such as if the PHI is related to a service or product for which the individual has paid out of pocket in full. A CE may break an agreed-upon restriction if the PHI is needed for emergency treatment or if the CE informs the individual in writing. Acceptance, denial, and/or termination of a restriction must be documented by the CE. DoD 6025.18-R, paragraph 10.1, provides information on the process and procedures to be followed by an individual in submitting a restriction request and by a DoD CE receiving such a request. Under revisions to the HIPAA Privacy Rule that became effective in 2013, additional rights to request restrictions were put in place, and are applicable to DoD CEs even though not yet referenced in a DoD issuance. These new rights are set out in Section 164.522 of the HIPAA Privacy Rule.



RIGHT TO AN ACCOUNTING OF DISCLOSURES

Individuals have a right to know to whom a DoD CE disclosed their PHI during a specific time period – up to six years prior to the date of the request. However, a DoD CE is not required to account to an individual for the following PHI disclosures:

- To carry out TPO
- To patients about their PHI
- Pursuant to the individual's written and signed authorization
- For the facility's directory and to persons involved in the individual's care or other notification purposes (disclosures permitted with the individual's opportunity to agree or object)
- For national security or intelligence purposes
- To correctional institutions or law enforcement officials
- Incidental to permitted uses or disclosures
- Made as part of a limited data set



MHS NoPP

The current MHS NoPP was issued by the DHA Privacy Office on October 1, 2013. The NoPP was written to enhance clarity and readability and to reflect the HIPAA Omnibus Final Rule modifications to the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule. It is important for beneficiaries and MHS workforce members to read the NoPP and understand their rights and our obligations as the MHS. The NoPP is also available in Braille, Arabic, Chinese, French, German, Italian, Japanese, Korean, Polish, Portuguese, Russian, Spanish, Tagalog, Thai, Turkish, and Vietnamese. For a complete listing of the different print options, along with more information, please see: <http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS/Notice-of-Privacy-Practices>.

CEs must respond within 60 days of the request. A CE may extend up to 30 days, to a date certain, and must provide the patient with an explanation for the extension in writing. These response timelines do not apply if temporary suspension of the individual's right is justifiably directed by the agency receiving disclosures under the health oversight or law enforcement exceptions, and it is documented. DoD 6025.18-R, Chapter 13, provides information on the process and procedures to be followed by an individual in requesting a disclosure accounting and by a DoD CE receiving such a request. In reporting accountable disclosures, the CE must include accountable disclosures by its BAs.

Individuals are entitled to one disclosure accounting in a 12-month period at no charge but a CE may charge a reasonable cost-based fee for additional requests, with prior notice to patient.

RIGHT TO REQUEST AN AMENDMENT

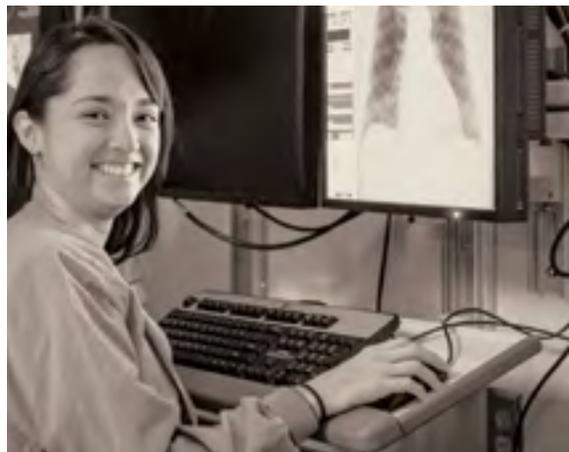
Individuals have the right to request an amendment to their PHI maintained in a designated record set. A CE may require such requests to be made in writing and must respond within 60 days. One 30-day extension is permitted if the individual is notified. If the request is accepted, the CE must make the amendment or addition to the record. A CE may deny a request if the PHI:

- Was not created by the CE, unless the individual provides reasonable basis to believe that the originator of the PHI is no longer available to act on the request
- Is not part of the designated record set
- Would not be available for inspection under the individual's right to inspect and copy
- Is accurate and complete

If the request is denied, the CE must provide a written statement to the individual and explain their right to file a written statement of disagreement. DoD 6025.18-R, Chapter 12, provides information on the process and procedures to be followed by an individual in submitting a request to amend and by a DoD CE receiving such a request.

CUSTODIAL AND NONCUSTODIAL PARENTS

A minor's personally identifiable information (PII)/PHI may be released to either parent, unless the CE is provided a legal documentation potentially affecting parental authority with respect to the minor's health care. In that situation, the CE should review the documentation to verify which parent has authority with respect to the minor's health care and whether disclosure of the minor's PHI to either parent is restricted. DoD 6025.18-R, paragraph C8.7, sets forth how DoD CEs determine who is the personal representative of a minor, as well as of adults and emancipated minors under applicable law, including applicable State law.





POINTS OF CONTACT

dha.ncr.pcl.mbx.
dha-privacy-office-mail@mail.mil
for HIPAA Privacy-related questions

dha.ncr.pcl.mbx.
privacy-office-materials@mail.mil
for DHA Privacy Office materials

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on HIPAA Privacy.

HIPAA Privacy Web Page

<http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS>

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
(currently under revision)

HIPAA Privacy Rule

45 CFR Parts 160 and 164

HIPAA SECURITY

Putting the HIPAA Security Safeguards to Work

The basic purpose of the HIPAA Security Rule is to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)¹ when it is stored, maintained, or transmitted. Complying with HIPAA Security Rule business practices and information technology safeguards help medical facilities endure threats and hazards to ePHI on a daily basis.

WHO IS COVERED?

HIPAA COVERED ENTITIES (CEs)	EXAMPLES IN THE DoD
Healthcare providers (including mental health) that transmit health information electronically in connection with certain transactions (such as claims)	Military treatment facilities (medical/dental)
Individual and group health plans	TRICARE Health Plan
Healthcare clearinghouses	Companies that perform electronic billing on behalf of military treatment facilities
Business associates (BAs)	Healthcare services support contractors and other contractors that provide services that require access to protected health information (PHI)

RISK MANAGEMENT AND THE HIPAA SECURITY RULE

The HIPAA Security Rule requires CEs and BAs to “reasonably and appropriately implement the standards and implementation specifications” taking into account several factors, including “the probability and criticality of potential risks to ePHI.”

This risk-based approach requires CEs and BAs to have an understanding of their technical capabilities, internal and external sources of ePHI, and known or potential threats and vulnerabilities in their environments.

¹ ePHI is PHI in electronic form that is transmitted or maintained by electronic media. Information transmitted by traditional fax or by voice over the telephone or by paper copy is PHI. These materials are generally not considered ePHI.



To assist HIPAA Security Officers in assessing reasonable and appropriate safeguards, the Privacy Overlays have been developed to identify minimum protections for ePHI. The Privacy Overlays link security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, to each HIPAA Security Rule standard and implementation specification.²

As organizations conduct HIPAA risk assessments, they may find that more stringent controls are appropriate than those that have been identified in the Privacy Overlays. Nothing in the Privacy Overlays prohibits organizations from applying more stringent controls to safeguard ePHI based on the results of their risk analysis. Conversely, the risk analysis may identify certain controls that are not applicable. For example, a system that merely stores appointment information will still fall under the protection of HIPAA, but may not need the same set of security and privacy controls

i KEY ELEMENTS OF RISK ANALYSIS

- ✓ Identify and document reasonably anticipated and potential threats specific to the operating environment
- ✓ Identify vulnerabilities which, if exploited by a threat, would create a risk of an inappropriate use or disclosure of ePHI
- ✓ Determine and document the potential impacts and risks to the confidentiality, integrity, and availability of ePHI
- ✓ Assess existing security measures
- ✓ Periodically review the risk analysis and update findings

that would be appropriate for an electronic health records system. Organizations should seek legal counsel if they are considering tailoring or otherwise altering the security and privacy controls identified in the Privacy Overlays.

² For additional information on the Privacy Overlays, refer to the Privacy Overlays section of this training manual.

THE HIPAA SECURITY RULE SAFEGUARDS

Administrative safeguards are designed to protect ePHI and to manage the conduct of DoD CE's workforce using ePHI in the performance of their jobs. There are nine administrative safeguards identified in DoD 8580.02-R, which is currently in the final stages of processing and nearing signature and publication as a revised DoD Instruction.

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- BA Contracts and Other Arrangements
- Evaluation

The Security Management Process is a crucial standard within the HIPAA Security Rule and contains the implementation specifications of Risk Analysis and Risk Management. These two specifications “form the foundation upon which an entity’s necessary security activities are built.”

For the Information Access Management standard, the policies and procedures adopted for addressing the Information Access Management standard must be guided by DoD 6025.18-R.

DoD 8580.02-R requires, at a minimum, annual technical and non-technical security evaluations. These evaluations are based initially on the standards implemented under the Regulation and subsequently changed in response to environmental or operational changes affecting the security of ePHI.

Annual security evaluations should include a review of the organizational safeguards, policies, and procedures in place, as well as a review of the security of the information systems and data.

Physical safeguards are “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

The Access Control and Validation Procedures specification requires policies and procedures for determining a person’s identity, as well as controlling a person’s access based on his/her job role. This may include implementing measures such as sign-in and/or escort for visitors to the areas of the facility that house information systems, hardware, or software containing ePHI.



The Maintenance Records specification requires DoD CEs to keep records of all repairs performed at a facility, including who performed them, what was done, and when it was done. This includes implementing policies and procedures to document repairs and modifications to the physical components of a facility that are related to security, such as hardware, walls, doors, and locks.

According to the Accountability specification of the Device and Media Controls standard, DoD CEs must implement procedures to maintain logs, including maintenance of records to keep track of who has the devices or media, when they had possession, and where they kept the devices or media from the time of original receipt to the time of final disposal or transfer to another person or entity.

Technical safeguards are the technology and policies and procedures for the use, protection, and access to ePHI.

- Access Controls
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Access Controls carry out the implementation of the Information Access Management standard, which set the rules on which workforce members can and should have access to the different types of data, how much data they should access (in accordance with the Minimum Necessary Rule), and what privileges they should have (read, write, etc.) in order to perform job functions.

Because electronically stored information can be lost, stolen, damaged, or destroyed if stored improperly or when equipment is moved, implementation specification for Data Backup and Storage requires that DoD CEs “create retrievable, exact copies of ePHI, when needed, before movement of equipment.”

DoD 8580.02-R does not require DoD CEs to protect unsolicited inbound transmissions, such as e-mail from patients. However, as required by Assistant Secretary of Defense for Health Affairs (ASD(HA)) Memorandum, “Military Health System (MHS) Information Assurance (IA) Policy Guidance and MHS IA Implementation Guides”, 23 February 2010, MHS personnel shall not transmit sensitive information or PHI via the Internet/e-mail or other electronic means unless appropriate security controls (e.g., encryption, Public Key Infrastructure) are in place.



STOP AND THINK - SECURITY TIPS

- ✓ Pay attention to the data you receive and share
- ✓ Always identify and label PHI as required
- ✓ Never use personal devices for official work
- ✓ Double check e-mail addresses before sending
- ✓ Only use authorized networks
- ✓ Report security incidents and breaches immediately
- ✓ Always encrypt e-mails that contain PHI (and PII)



POINT OF CONTACT

dha.ncr.pcl.mbx.hipaa-security@mail.mil
for HIPAA Security-related questions

RESOURCES

HIPAA Security Web Page

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS>

HIPAA Security Rule

45 CFR Parts 160, 162 & 164

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
(currently under revision)

DoD Health Information Security Regulation

DoD 8580.02-R, July 12, 2007
(currently under revision)

ASD Memorandum

Disposition of Unclassified DoD Computer Hard Drives, June 4, 2001

ASD for Health Affairs Memorandum

MHS IA Policy Guidance and MHS IA Implementation Guides, February 12, 2010

Security Controls for Federal Information Systems and Organizations

NIST SP 800-53, Revision 4, April 2013

PRIVACY OVERLAYS

Integrating Security Standards

With DoD's ongoing alignment with the National Institute of Standards and Technology (NIST) security controls, the DHA Privacy Office has continued to work on ways to better integrate HIPAA Security with existing DoD cybersecurity standards. This integration will help provide clarity and enhance overall HIPAA Security compliance.

The DHA Privacy Office has participated in an effort to further develop the necessary electronic protected health information (ePHI) specific guidance on this transition through the Committee on National Security Systems (CNSS) Privacy Overlays Working Group. The CNSS Privacy Overlays Working Group is one of several government working groups that develops tools to fashion privacy-specific controls into and onto the larger context of system security controls.

The Privacy Overlays are a specification of privacy-centric security controls, to include supporting guidance used to complement the security control baseline selection according to DoD policy, and the supplemental guidance found within the NIST "Security and Privacy Controls for Federal Information Systems and Organizations". The Privacy Overlays are used as a tool by information systems security engineers, authorizing officials, privacy officials, and others to select appropriate protections for differing privacy information types, including ePHI.

Noticeably included within this new tool is a feature that allows privacy officials and cybersecurity experts the ability to align existing

privacy/security requirements applicable to a specific computing system containing ePHI. The use of the Privacy Overlays alongside NIST security control baselines allow security and privacy controls to be customizable and implemented as part of an organization-wide process that manages cybersecurity and overall privacy risk.



PRIVACY OVERLAYS FRAMEWORK

- NIST Special Publication (SP) 800-53, Revision 4, Security Controls for Federal Information Systems and Organizations, April 2013
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010
- Committee on National Security Systems Instruction (CNSSI) No. 1253, March 27, 2014
- Privacy Act of 1974, as amended (5 U.S.C. 552a)
- E-Government Act of 2002 (P.L. 107-347)



The Privacy Overlays apply to information systems and organizations that maintain, collect, use, or disseminate PII, including ePHI. These types of privacy-centered overlays support privacy programs, system owners, program managers, developers, and those who maintain information systems by identifying security and privacy controls and requirements. They also serve as a tool to develop guidance and privacy best practices.

HOW DOES IT WORK?

Not all PII must be protected equally. NIST SP 800-122, Guide to Protecting the Confidentiality of PII, provides a methodology to both categorize

PII and determine the PII confidentiality impact level. Based on the sensitivity of PII in the system – low, moderate, or high – the methodology indicates the potential harm that could result if PII was inappropriately accessed, used, or disclosed.

The PII confidentiality impact level is used to determine which security and privacy controls apply to a given system. While this may appear similar to the impact values for the security objectives of a system (confidentiality, integrity, and availability), it is very different. The system security objectives are used to determine the security control baselines in CNSSI No. 1253.



POINT OF CONTACT

dha.ncr.pcl.mbx.hipaa-security@mail.mil
for Privacy Overlays-related questions

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on the Privacy Overlays.

Categorization and Control Selection for National Security Systems

CNSSI No. 1253, March 27, 2014

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

NIST SP 800-122, April 2010

Security Controls for Federal Information Systems and Organizations

NIST SP 800-53, Revision 4, April 2013

Cybersecurity

DoD Instruction (DoDI) 8500.01,
March 14, 2014

Risk Management Framework (RMF) for DoD Information Technology (IT)

DoDI 8510.01, March 12, 2014

DoD Health Information Security Regulation

DoD 8580.02-R, July 12, 2007

(currently under revision)

Protected health information (PHI) is a subset of PII that comes with a distinct set of applicable laws and regulations. In addition to those that apply to all types of PII, the Privacy Overlays distinguish between PII and PHI to clearly document the supplemental guidance, control extensions, and regulatory and statutory references that apply specifically to PHI (i.e., the HIPAA Privacy and Security Rules).¹ PHI is, by definition, PII and the laws, regulations, and other standards for safeguarding PII also apply to PHI. Therefore, the organization must follow the guidance contained in the Privacy Overlays to determine the PII confidentiality impact level of the information it owns or manages and apply the appropriate subpart of the Privacy Overlays (i.e., low, moderate, or high). After determining the PII confidentiality impact level, the organization must also consider the guidance related to PHI within the Privacy Overlays.

¹The PHI subpart of the Privacy Overlays applies to all federal government agencies that adopt CNSSI No. 1253 and are covered entities or business associates.

HIPAA TRANSACTIONS, CODE SETS, AND IDENTIFIERS

HIPAA Compliance

The HIPAA Administrative Simplification provisions required the Department of Health and Human Services to establish national standards for electronic healthcare transactions, code sets, and identifiers (TCS&I). National standards for HIPAA TCS&I improve the effectiveness and efficiency of the healthcare industry by simplifying the administration of the system and enabling the efficient electronic transmission of certain health information.

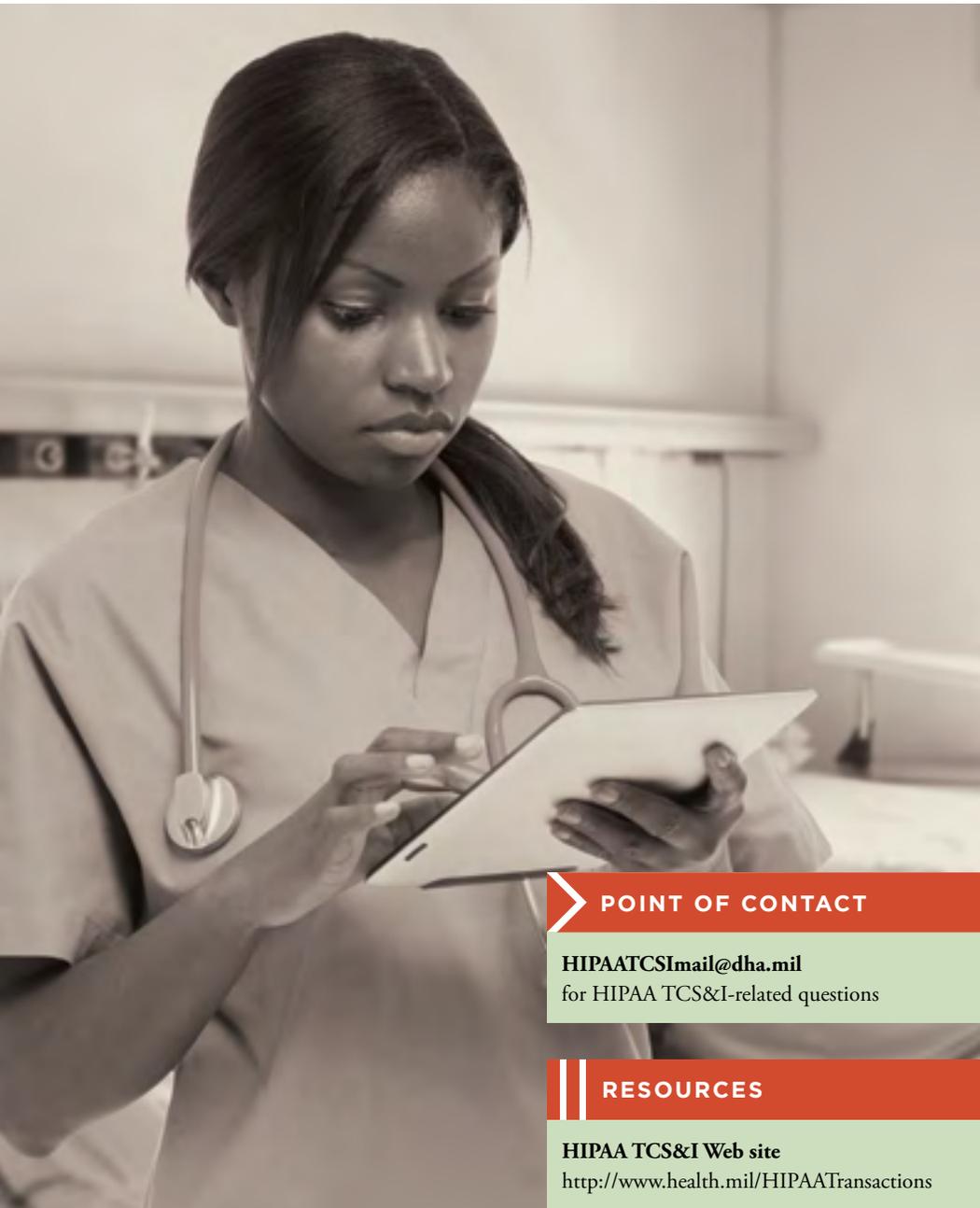
While the DHA Privacy Office supports MHS compliance with HIPAA Privacy and Security Rules, DHA's Business Support Directorate/ Business Information Management Office facilitates MHS HIPAA TCS&I Rules compliance. To date, rules for HIPAA TCS&I have come from both the HIPAA legislation as well as from the Patient Protection and Affordable Care Act (also known as ACA). These mandate standards that must be used when conducting named and adopted HIPAA electronic administrative healthcare transactions such as enrollment in a health plan, eligibility checking, referrals, and claims processing. HIPAA-mandated identifiers include the Employer Identifier, the National Provider Identifier, and the Health Plan Identifier. These identifiers are used within HIPAA transactions to identify employers, providers, and health plans.

HIPAA also mandates the use of certain code sets within HIPAA transactions. For example, ICD-10 (the International Classification of Diseases,

10th Revision, Clinical Modification (CM) and Procedure Coding System (PCS)) are code sets required by HIPAA. HIPAA TCS&I standards affect TRICARE, both as a HIPAA-covered health plan and as a provider of healthcare services.

WHICH COVERED ENTITIES NEED TO COMPLY?

- Providers (e.g., hospitals, civilian clinics, and military treatment facilities), individuals (e.g., physicians) and group provider practices
- Health plans (e.g., TRICARE, Blue Cross/Blue Shield)
- Clearinghouses (e.g., ePremise, Emdeon)
- Business associates of the covered entities (e.g., Defense Manpower Data Center/ Defense Enrollment Eligibility Reporting System, and Managed Care Support Contractors)



POINT OF CONTACT

HIPAAATCSImail@dha.mil
for HIPAA TCS&I-related questions

RESOURCES

HIPAA TCS&I Web site
<http://www.health.mil/HIPAATransactions>

DATA SHARING

Requesting Access to Data Managed by DHA

The DHA Privacy Office receives various types of data sharing requests for MHS data that is owned or managed by DHA. Under its Data Sharing Program, the Privacy Office reviews each request for compliance with applicable federal and DoD regulatory requirements. Parties involved in the requested use or disclosure of DHA data must comply with all applicable standards and safeguard the integrity of the data received.

DATA SHARING AGREEMENT (DSA) PROGRAM

The Privacy Office uses the DSA process to:

- Confirm that any requested use/disclosure of DHA data is permitted or required by applicable DoD regulations and privacy laws
- Promote privacy-associated accountability in the MHS
- Maintain DSA records to confirm the covered entity's compliance in case of an investigation
- Meet certain compliance requirements, such as:
 - Making reasonable efforts when disclosing data to limit the information to the minimum necessary for achieving the intended purpose
 - Abiding by information protection regulations

DATA SHARING AGREEMENT APPLICATION (DSAA)

An application, designed by the Privacy Office, as a tool to accomplish the following objectives before a DSA will be executed to:

- Obtain satisfactory assurance that the requested data will be appropriately safeguarded
- Verify that the requested data use is endorsed by the data owner (e.g., system program office)



The DSAA also allows the Privacy Office to confirm the following key compliance points:

- The requested data will be used according to the permitted uses defined in the appropriate System of Records Notice
- Information system(s) and networks intended for data processing and/or storage have appropriate physical, administrative, and technical safeguards
- Research-related data use requests have been reviewed by the appropriate compliance offices and obtained the related determinations, including the Institutional Review Board (IRB), the DHA Human Research Protection Program (HRPP), and the DHA Privacy Board

i A DSAA MUST BE INITIATED BY THE FOLLOWING:

Applicant – The individual who will provide primary oversight and is responsible for the handling of the requested data.

- For contract-driven requests, must be an employee of a prime contractor
- For projects with more than one prime contractor, must be completed by each prime contracting organization that will have custody of the requested data

Government Sponsor – The point of contact within DHA or the respective Armed Service who assumes responsibility for the contract, grant, project, or Cooperative Research and Development Agreement.

Once all compliance reviews are completed and the DSAA is approved by the DHA Privacy Office, one of the following DSAs will be executed based on the type of data requested:

- DSA for de-identified data
- DSA for personally identifiable information (PII), excluding protected health information (PHI)
- DSA for limited data set, known as a Data Use Agreement
- DSA for PHI

i THE RESEARCH DATA SHARING STREAMLINING MEASURES ARE:

1. Create uniform MHS-wide HIPAA research templates and guidance
2. Develop issuances that set conditions under which the DHA Privacy Board review may no longer be required for participating enhanced multi-service markets (eMSMs)
3. Eliminate the need for government personnel seeking data for research purposes to submit a DSAA and enable DoD IRBs or HIPAA Privacy Boards to monitor HIPAA research compliance
4. Maintain the DSAA requirement for research-related contractors; however, no longer require DHA Privacy Board review for studies within eMSMs working with the DHA Privacy Office
5. Accept an overarching DSAA from research organizations exclusively conducting research within participating eMSM without needing a DSAA from each individual researcher

RESEARCH DATA SHARING STREAMLINING INITIATIVES

Streamlining measures are currently underway to prepare some eMSMs for their MHS IRB or HIPAA Privacy Boards to take on the responsibility of conducting the required HIPAA Privacy Rule reviews and generating appropriate HIPAA-compliant documentation.

DHA PRIVACY BOARD

The DHA Privacy Board reviews research-related requests for PHI owned or managed by DHA for compliance with the HIPAA Privacy Rule.

There are four types of Privacy Board reviews:

1. Studies that must obtain HIPAA authorizations from each participant. The Board will review the proposed authorization for HIPAA compliance
2. Studies that require Waivers of Authorization or Altered Authorizations. Waivers are required when it is not possible or practicable to get authorizations from all study participants. Altered Authorizations are required for studies where it is not possible to include all of the statements HIPAA requires researchers to include in authorizations or when it is not possible to get signed authorizations
3. Studies that only perform research on the PHI of decedents must submit the Required Representations for Research on Decedent's Information
4. Studies that require access to or use of PHI solely for preparing a research protocol or similar pre-study activity must submit the Required Representations for Review Preparatory to Research. This cannot be used if the researcher plans to remove PHI from DHA or to contact individuals during these pre-study activities



ARE YOU READY TO SUBMIT YOUR REQUEST?

- ✓ Have you completed the most current DSA request template?
- ✓ Have you adequately described the process intended to receive, use, de-identify, store, publish, and/or report the data?
- ✓ Do you have all other applicable compliance approvals required for this data use?
- ✓ Have you included the appropriate Data Request Template, if needed?
- ✓ Did both the Applicant and Government Sponsor sign or initial the request?





POINTS OF CONTACT

DSA.Mail@dha.mil

for DSA-related questions

DHAPrivBrd@dha.mil

for DHA Privacy Board-related questions

dha.ncr.pcl.mbx.

dha-privacy-office-mail@mail.mil

for HIPAA Privacy-related questions

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on Data Sharing Agreements.

DSA Web Page

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Submit-a-Data-Sharing-Application>

DHA Privacy Board Web Page

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Board>

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
(currently under revision)

DoD Health Information Security Regulation

DoD 8580.02-R, July 12, 2007
(currently under revision)

HUMAN RESEARCH PROTECTION PROGRAM

Research Compliance

DoD supports and encourages research, including human subject research, in order to continue to improve and enhance medical science and health care for all MHS beneficiaries. All research protocols that include human subjects must be compliant with federal laws, federal regulations, and DoD policies intended to protect the subjects of the studies. The Human Research Protection Program (HRPP) provides guidance and enhances collaboration on research compliance issues.

HRPP COMPLIANCE REVIEWS

The HRPP reviews compliance with:

- Department of Health and Human Services (HHS) Regulation, “Protection of Human Subjects”, 45 Code of Federal Regulations (CFR) 46, the “Common Rule”
- 32 CFR 219, “Protection of Human Subjects” (DoD’s adoption of the “Common Rule”)
- DoD Instruction (DoDI) 3216.02, “Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research”
- 10 United States Code 980, “Limitations on Use of Humans as Experimental Subjects”

The Human Research Protection Official reviews studies that are approved by Institutional Review Boards (IRBs) with federal-wide assurance from HHS and agreement with DHA attesting to its understanding of and adherence to DoD-specific protections, and includes:

- Initial review of approved protocols
- Requests to modify previously approved protocols

- Requests to continue a study beyond the expiration date of a previous approval

The HRPP Office reviews protocols to determine if they meet the criteria for research involving human subjects and if so, conducts reviews to determine whether the research is exempt from IRB review. If exempt, the HRPP Office reinforces the understanding that the investigators



HRPP COMPLIANCE REVIEWS

HRPP compliance reviews are required for research involving human subjects and all protocols must be submitted through a single, web-based protocol submission tool that has been adopted for use with all Defense Health Program (DHP) funded studies. This system can be used for non-DHP funded studies as well. Investigators can access the system at http://fhpr.dhhq.health.mil/resources/research-regulatory-oversight/dmrn_access.aspx

must adhere to the ethical standards set forth in the Common Rule in order to provide research subjects with the greatest protection from harm.

The HRPP further works with the DHA Privacy Board in reviewing research studies requiring data owned and/or managed by DHA for compliance with the HIPAA Privacy Rule.

HRPP TRANSITION

HRPP transitioned in mid-2011 from the Defense Health Cost Assessment and Program Evaluation to the DHA Privacy and Civil Liberties Office.



POINT OF CONTACT

TMA_HRPP@dha.mil
for HRPP-related questions

RESOURCES

HRPP Web Site

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Protect-Humans-in-Research>

Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research

DoDI 3216.02, March 2002
(currently under revision)

BREACH RESPONSE

Prevention and Mitigation

Equip yourself with a clear understanding of what breaches are, why they occur, and how to prevent them—it is the key to compliance with the Privacy Act of 1974 and HIPAA, when faced with a potential violation. Mishandled or misused personally identifiable information (PII) or protected health information (PHI) can result in a breach or HIPAA Privacy violation, but the tips in this chapter can serve as a quick reference for methods on how to prevent breaches and on how to mitigate breaches if they occur.

WHAT IS A BREACH?

UPDATED Under the Privacy Act and as defined by DoD, a breach is “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 an other than authorized purpose, have access or potential access to PII, whether physical or electronic.” (*Revised definition as of October 29, 2014*)

Under HIPAA and as defined by the Department of Health and Human Services (HHS), an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

i TOP MHS BREACH TRENDS FOR FISCAL YEAR 2014

1. Misdirected postal mail
2. Misdirected fax
3. Unencrypted e-mail
4. Misdirected e-mail
5. Unauthorized access and disclosure (human error)
6. Loss of records
7. Theft





BREACH PREVENTION TIPS

- Verify the recipient's contact information (e-mail address, mailing address, fax number, etc.) before sending correspondence
- Do NOT leave government equipment in your vehicle in plain view
- Properly package and seal correspondence prior to mailing
- Encrypt all e-mails that contain sensitive information
- Ensure all sensitive information is de-identified or completely removed when used in presentations or publications
- Properly shred all documentation prior to disposal
- Remove documents from the printer immediately, if used in a shared environment
- Establish and routinely check role-based access to data and information
- Enforce consequences for employees who access and disclose information without authorization
- Create a workplace culture focused on privacy and security
- Train. Train! Train!!
- Require annual Privacy Act and HIPAA training
- Require refresher/remedial training to mitigate a breach
- Ensure reminder banners appear upon access of systems containing PII/PHI
- Include breach awareness posters in break rooms and high traffic areas

BREACH REPORTING

Upon discovery of an actual or possible breach, reporting must take place in accordance with the local incident response protocol.

FOR DHA	FOR SERVICE COMPONENTS
LEADERSHIP: Immediately	LEADERSHIP: Immediately
US COMPUTER EMERGENCY READINESS TEAM: Within 1 hour of a confirmed cyber security incident*	US COMPUTER EMERGENCY READINESS TEAM: Within 1 hour of a confirmed cyber security incident*
DHA PRIVACY & CIVIL LIBERTIES OFFICE: Within 1 hour of discovery	DoD COMPONENT SENIOR PRIVACY OFFICIALS: Within 24 hours of discovery
DEFENSE PRIVACY & CIVIL LIBERTIES DIVISION: Within 48 hours**	DHA PRIVACY & CIVIL LIBERTIES OFFICE: Within 24 hours of discovery
DEPARTMENT OF HEALTH AND HUMAN SERVICES*: Within 60 days of discovery if 500 or more individuals are impacted Within 60 days of the close of the calendar year if less than 500 individuals are impacted	DEFENSE PRIVACY & CIVIL LIBERTIES DIVISION: Within 48 hours***

*US-CERT reporting is no longer required for non-cyber related incidents (e.g. paper breaches).

**DHA is responsible for reporting to the Defense Privacy and Civil Liberties Division (DPCLD) and the Secretary of HHS.

***The Service Components are responsible for reporting up their chain of command and to DPCLD.

NOTE: If necessary, notify issuing banks (if government issued credit cards are involved); law enforcement; and all affected individuals within 10 working days of breach discovery and the identities of the impacted individuals that have been ascertained.

THE SEVEN STEPS TO AN EFFECTIVE BREACH RESPONSE PLAN

1. BREACH IDENTIFICATION

Recognize that an event has occurred and initiate next step

- Gather all available information and make required assessments
- Confirm and classify the scope, risk, and severity of the breach
- Determine an appropriate plan of action

2. BREACH REPORTING

Report the breach to the established chain of command in a timely manner

- Notify supervisor immediately and initiate the appropriate reporting steps
- Notify the Information/System Owners, and the appropriate Program Office of the breach

3. CONTAINMENT

Limit the impact of the breach

- For electronic breaches, determine a course of action concerning the operational status of the compromised system, and identify the critical information and/or computing services affected
- For non-electronic breaches, identify the best strategy to minimize the impact of the breach

4. MITIGATION

Communicate with potentially affected individuals, investigators, and other involved entities. Additional actions may include:

- Immediately securing the affected information as much as practicable
- Applying appropriate administrative, physical, and technical safeguards

i DHA ADMINISTRATIVE INSTRUCTION 71, "INCIDENT RESPONSE TEAM AND BREACH RESPONSE REQUIREMENTS," SIGNED JUNE 6, 2014

The revised Administrative Instruction (AI) outlines the processes and procedures for individuals and supervisors responsible for assessing and responding to a confirmed or suspected breach that occurs within DHA. It also continues the requirement to annually convene an Incident Response Team for training purposes. This year's exercise was held on March 17, 2015.

NOTE: AI 71 only applies to DHA workforce members; however, it may be used as a reference by the Services and Purchase Care Contractors.

i CHANGES TO US-CERT REPORTING REQUIREMENTS

On February 20, 2015, DoD issued changes to the US-CERT reporting requirement in accordance with the Department of Homeland Security's US-CERT Federal Incident Notification Guidelines, dated January 14, 2015. According to these changes, all federal agencies are required to only report confirmed cyber related incidents to US-CERT within one hour. Non-cyber related breaches (e.g. paper breaches) should no longer be reported to US-CERT.

NOTE: The above change only applies to US-CERT reporting. All breaches (cyber and non-cyber related) must still be reported to the DHA Privacy Office and DPCLD, as required.

5. ERADICATION

Remove the cause of the breach and alleviate vulnerabilities. Examples of such actions may include:

- Deleting any computer viruses
- Updating beneficiary contact information

6. RECOVERY

Restore business operations to normal status

- Execute the necessary changes to business practices and/or network/system and fully restore system and data

7. FOLLOW-UP

Take necessary actions to prevent future occurrences

- Ensure all tasks in the mitigation strategy are completed
- Share lessons learned and amend operational policies as needed
- Take appropriate personnel actions, e.g., counseling and sanctioning

BREACH POLICIES AND PROCEDURES

Appropriate policies and procedures are critical for breach prevention and to have an effective response management plan. Policies and procedures should include:

- Accessing, using, and disclosing PII/PHI
- Safeguarding PII/PHI
- Breach reporting
- Comprehensively documenting communications, requests, and findings
- Requiring HIPAA Privacy and Security training

Awareness of the applicable privacy and security policies can be achieved when information is thoroughly disseminated to staff members, and staff members are then notified and trained appropriately on policy changes or updates.

COMPLIANCE ENFORCEMENT

Enforcement of compliance is vital to breach prevention and should be reviewed with staff members regularly. If little or no consequences will be executed for breaching PII/PHI, staff members will be less likely to take compliance seriously. Therefore, the following tips are recommended:

- Include consequences and/or penalties for staff member non-compliance in employee manuals
- Re-train and provide remedial training on the appropriate privacy policies
- Consider stiffer penalties such as suspension, revocation of access, and/or termination
- Consistently promote awareness to prevent violations and breaches

WORKFORCE TRAINING

Enforcement of staff training is essential to ensure compliance with the appropriate privacy and security policies. Therefore, the following tips are recommended:

- Confirm staff members are not only current with their annual Privacy Act and HIPAA training, but also have relevant job-specific training
- Ensure staff members have completed required remedial training
- Investigate whether job-specific training is available and work with your local Privacy Office to ensure your staff members are trained appropriately



POINTS OF CONTACT

**dha.ncr.pcl.mbx.
dha-privacy-officer@mail.mil**
to report breaches and for breach-related questions

**dha.ncr.pcl.mbx.
dha-privacy-office-mail@mail.mil**
for HIPAA Privacy-related questions

dha.ncr.pcl.mbx.hipaa-security@mail.mil
for HIPAA Security-related questions

RESOURCES

Enclosed CD
Please see enclosed CD for detailed presentation on Breach Response and Prevention.

Breach Response Web Page
<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI>

HIPAA Privacy Web Page
<http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS>

EXTERNAL COMPLIANCE OVERSIGHT

Audits Under HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires the Department of Health and Human Services (HHS), through the Office for Civil Rights (OCR), to conduct periodic audits to ensure covered entities (CEs) and business associates (BAs) comply with the HIPAA Privacy, Security, and Breach Notification Rules.

Expansion and broad implementation of the HHS HIPAA audit program did not occur in 2014, as planned, because of a delay in the rollout of the technology used to collect audit-related documents from CEs and BAs. However, in January 2015, the OCR Director stated “OCR is committed to implementing an effective audit program, and audits will be an important compliance tool for OCR.”

CEs and BAs can prevent the loss of contracts, civil and criminal investigations, civil money penalties, and other adverse results (that may result from an HHS audit) by conducting robust reviews and assessments, mapping the movement of protected health information (PHI) within their organizations, and complying with HHS guidance.

GETTING READY FOR AN AUDIT

The Army, Navy, Air Force, DHA healthcare providers, military treatment facilities (MTFs), and the DoD health plans are within the MHS and regulated by HIPAA. Certain U.S. Coast Guard components are also part of an organized health care arrangement within the MHS and must comply with the HIPAA Rules. Whether OCR will select any DoD CE or one of their BAs for a HIPAA audit in 2015 or beyond, is unknown. However, DoD CEs and their BAs may lower their risks, improve their overall compliance with the HIPAA Rules, position themselves

OCR'S HITECH AUDIT PROGRAM GOALS

- Identify best practices
- Proactively uncover risks and vulnerabilities
- Provide a proactive and systematic means to assess and improve industry compliance
- Enhance industry awareness of compliance obligations
- Enable OCR to target its outreach and technical assistance to identified problems and to offer tools to the industry for self-evaluation and prevention

to better withstand an investigation that may result from a HIPAA complaint, and improve their safeguards protecting the confidentiality, integrity, and availability of PHI by assuming they will be selected for a HIPAA audit. If this

assumption is made, steps can be taken to assure their HIPAA safeguarding efforts are in order.

PHI management and compliance steps that are recommended for DoD CEs and their BAs include:

- Ensuring you have the documentation required by the HIPAA Privacy and Security Rules, as implemented by DoD 6025.18-R and DoD 8580.02-R standards and specifications
- Mapping information security controls to the HIPAA Security Rule and DoD 8580.02-R standards and specifications
- Confirming a risk assessment has been conducted within the past 12 months and the resulting risk management plan is available
- Ensuring a continuity of operations plan is available
- Mapping your existing internal organizational procedures demonstrating full compliance with HIPAA Privacy Rule provisions
- Reviewing the HIPAA Omnibus Final Rule issued by HHS in January 2013, which became effective in late September 2013, and the changes it made to the HIPAA Privacy, Security, and Breach Notification Rules. Use that review, as well as DHA Privacy Office breach notification guidance, to determine the changes, if any, needed to your organization's internal compliance procedures and processes. Then, make and document the necessary changes. For MTFs, ensure you have documented how your organization handles

TOP PRIVACY AND SECURITY PROBLEMS FROM HHS HIPAA AUDIT PILOT PROGRAM

PRIVACY RULE	SECURITY RULE
Policies and procedures	User activity monitoring
Complaints	Contingency planning
Privacy training	Authentication/integrity
Mitigation of known harmful effects on non-compliance	Media reuse and destruction

access to or amendment of an individual's health information, alternative communications, restrictions on disclosures, and the accounting of disclosures

- Ensuring your workforce is appropriately trained in HIPAA Privacy and Security matters applicable to your organization/facility and its duties

POINT OF CONTACT

dha.ncr.pcl.mbx.
dha-privacy-office-mail@mail.mil
 for HIPAA compliance questions

RESOURCES

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
 (currently under revision)

DoD Health Information Security Regulation

DoD 8580.02-R, July 12, 2007
 (currently under revision)

MILITARY COMMAND EXCEPTION

Disclosing PHI of Armed Forces Personnel

In accordance with the HIPAA Privacy Rule, DoD 6025.18-R, and applicable DoD issuances, a DoD covered entity (CE) may use and disclose the protected health information (PHI) of individuals who are Armed Forces members for activities deemed “necessary by appropriate military command authorities to assure the proper execution of the military mission.” This is commonly referred to as the “Military Command Exception.” See paragraph C7.11.1.2 of the DoD 6025.18-R for information on who are considered “appropriate military command authorities”.

This exception explains when DoD providers may (1) disclose PHI of Service members to military commanders or (2) use PHI of Service members for military commanders’ purposes, such as evaluating fitness for duty. If the specific requirements of this exception are satisfied, patient authorization is not required for such uses or disclosures. Disclosures of PHI under the military command exception are

permitted, not required. Any disclosure of PHI to a commander under this exception is subject to the HIPAA Privacy Rule and DoD 6025.18-R. Although DoD 6025.18-R is not applicable to non-DoD CEs, the exception is stated in 45 CFR 164.512(k)(1)(i) and therefore, applies to non-DoD CEs, such as non-government hospitals and private healthcare providers.

MILITARY COMMAND AUTHORITY

- Commander with authority over a member of the Armed Forces
- Other person designated by such commander
- Designee of an appropriate Secretary or another official delegated authority by such Secretary

ARMED FORCES PERSONNEL

Attention is called to the Department of Health and Human Services’ Office for Civil Rights (OCR) limited scope of the term “Armed Forces personnel” as used in the HIPAA Privacy Rule’s military command exception. OCR interprets this term to be limited only to active members of the Armed Forces.

MILITARY COMMAND AUTHORITIES

Appropriate military command authorities include commanders who exercise authority over a member of the Armed Forces, or another person designated by such a commander to receive PHI to carry out an activity under that commander's authority.

Other appropriate authorities include any official designated for this purpose by the Secretary of Defense, the Secretary of the applicable Military Department, or the Secretary of Homeland Security (for Coast Guard activities not under the Navy).

FURTHER DISCLOSURES

Military commanders who receive PHI have special responsibilities to safeguard the information and limit any further disclosure in accordance with the Privacy Act of 1974 and the DoD Privacy Program as now or hereafter in effect.

PHIMT ASSISTANCE

For PHIMT assistance visit:
<http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Act-and-HIPAA-Privacy-Training>

ACCOUNTING OF DISCLOSURES

Disclosures to military commanders must be documented for disclosure accounting purposes. See DoD Instruction (DoDI) 6025.18 for guidance. Documentation is best accomplished by recording military command exception disclosures in the Protected Health Information Management Tool (PHIMT) at the time those disclosures are made.

WHAT IS "NECESSARY TO ASSURE PROPER EXECUTION OF THE MILITARY MISSION"?

Under paragraph C7.11.1.3 of DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 24, 2003, the military purposes for which PHI may be used or disclosed include:

1. Determining the member's fitness for duty, including but not limited to compliance with:
 - DoD Directive 1308.1, "DoD Physical Fitness and Body Fat Program", June 30, 2004;
 - DoDI 1332.38, "Physical Disability Evaluation", November 14, 1996 (incorporating Change 2, April 10, 2013); and,
 - DoDI 5210.42, "Nuclear Weapons Personnel Reliability Program", July 16, 2012
2. Determining the member's fitness to perform any particular mission, assignment, order, or duty, including any actions required as a precondition to performance
3. Carrying out comprehensive health surveillance activities in compliance with DoD Directive 6490.02E, "Comprehensive Health Surveillance", February 8, 2012
4. Reporting on casualties in connection with a military operation or activity in accordance with applicable military regulations or procedures
5. Carrying out other activities necessary to the proper execution of the Armed Forces' mission

The military command exception applies only to disclosures of active duty Armed Forces personnel PHI. PHI of family members or other categories of beneficiaries is never shared with military command authorities without a HIPAA-compliant authorization.

MENTAL HEALTH AND/OR SUBSTANCE MISUSE DISCLOSURES

To foster DoD's culture of support in the provision of mental health care and voluntarily sought substance abuse education to military personnel, DoDI 6490.08, "Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members", August 17, 2011, provides guidance regarding command notification requirements. This DoDI requires certain disclosures of mental health-related information to commanders, and prohibits other disclosures of mental health information to commanders. The requirements of DoDI 6490.08 apply only to DoD CEs; it does not apply to CEs outside of the MHS.

CEs shall not notify a Service member's commander when the member obtains mental health care or substance abuse education services, unless a certain condition or circumstance is met. See Enclosure 2, paragraph 3.b. of DoDI 6490.08.

In contrast to the HIPAA Privacy Rule, the Alcohol, Drug Abuse, and Mental Health Administration (ADAMHA) Reorganization Act regulations broadly permit the "interchange of that information within the Armed Forces"; however, the disclosure of PHI must satisfy both ADAMHA and the HIPAA Privacy Rule. Therefore, it is not sufficient that a disclosure by a military treatment facility (MTF) provider to a commander is a permitted "interchange . . . within the Armed Forces." The disclosure must separately comply with the HIPAA military command exception.

RECOMMENDED MTF POLICIES AND PROCEDURES

The following policies and procedures are recommended regarding the disclosure of Armed Forces members' PHI to appropriate military command authorities:

1. Designate person(s) at an MTF with authority to release PHI to commanders
2. Maintain documentation of commanders and other designees to whom Service members' PHI may be disclosed
3. Train personnel on circumstances where PHI disclosures to military command authorities are and are not appropriate
4. Educate personnel on the use of PHIMT to comply with disclosure accounting requirements

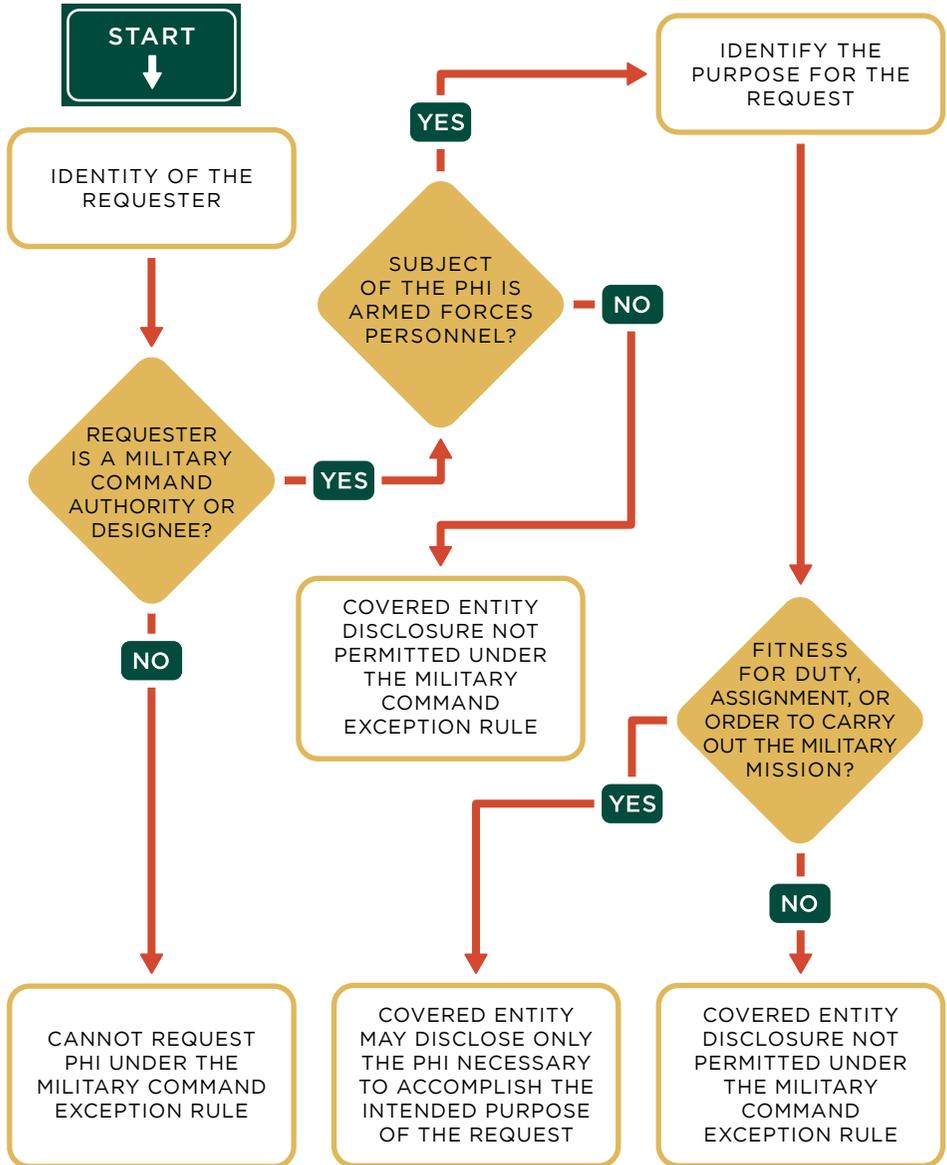


DISCLOSURE OF PHI RELATING TO MENTAL HEALTH CARE OR SUBSTANCE ABUSE TREATMENT

Command notification by CEs is not permitted for a Service member's self and medical referrals for mental health care or substance abuse education unless the disclosure is authorized under subparagraphs 1.b.(1) through 1.b.(9) of Enclosure 2. If one of those provisions applies, then notification is required.

Notifications shall generally consist of the diagnosis, a description of the treatment prescribed or planned impact on duty or mission, the recommended duty restrictions, and the prognosis.

MILITARY COMMAND EXCEPTION DISCLOSURES





POINT OF CONTACT

dha.ncr.pcl.mbx.

dha-privacy-office-mail@mail.mil

for questions regarding the HIPAA Privacy Rule and the Military Command Exception

RESOURCES

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
(currently under revision)

DoD Privacy Program

32 CFR Part 310, DoD Privacy Program,
80 CFR 4201, January 27, 2015;
DoDD 5400.11, October 29, 2014;
DoD 5400.11-R, May 14, 2007
(currently under revision)

Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members

DoDI 6490.08, August 17, 2011
(currently under revision)

HIPAA Privacy Web Page

<http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS>

DHA Privacy Military Command Exception Web Page

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS/Military-Command-Exception>

EMERGING TECHNOLOGY

Maintaining and Transmitting Electronic Health Data

DoD has been at the forefront of applying emerging technologies to health care for many years. Because of its ongoing need to exchange information with the Department of Veterans Affairs (VA) for over 9.6 million beneficiaries, DoD has been a leader in electronically sharing health data. To improve the quality of health care provided to beneficiaries, DoD has strived to increase the comprehensiveness of the data it exchanges along with expanding information sharing with other agencies and the private sector. DoD was one of the first organizations to deploy an electronic medical record and has played a key role in developing standards to allow systems to share usable data.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, not only required major changes in the HIPAA Privacy, Security, and Enforcement Rules, but also provided incentives to increase the adoption of electronic health records (EHR) that have served as a major emerging technology catalyst. Electronic data sharing is also being driven by the National Defense Authorization Act (NDAA) of 2014, which requires DoD and VA to deploy modernized EHR software by December 31, 2016. The NDAA also requires interoperability of DoD and VA EHR systems and the development of a Personal Health Record by the two Departments.

The rapid introduction of new technologies raises many significant privacy issues. DoD is developing information technology (IT) capabilities that include requirements to protect the privacy and security of data that it maintains, uses, and transmits. DoD is implementing electronic capabilities to control data uses and

“...I’m asking both departments to work together to define and build a seamless system of integration with a simple goal: When a member of the Armed Forces separates from the military, he or she will no longer have to walk paperwork from a DOD duty station to a local VA health center. Their electronic records will transition along with them and remain with them forever.”

President Barack Obama
April 9, 2009

disclosures that require consents or authorizations from individuals. The Department has embarked on several initiatives to establish data sharing guidelines and taken steps to set expectations about the use and further disclosure of data, once it is shared with both covered and non-covered entities. Specifically, DoD uses various types of Data Sharing Agreements, such as a Data Use

DoD EMERGING TECHNOLOGY INITIATIVES	GOALS
Health Information Exchange	<ul style="list-style-type: none"> • Increase electronic data sharing with both private and federal partners • Improve interoperability by implementing industry-wide standards • Improve quality of care by increasing data access • Exchange data for non-treatment purposes which are administrative in nature, such as benefits adjudication
Viewers (BHIE, FHIE, HAIMS, JLV)	<ul style="list-style-type: none"> • Consolidate current viewers into one MHS-wide viewer • Improve capability to see images • At a minimum, maintain the capabilities that exist in the current viewers
Electronic Health Record	<ul style="list-style-type: none"> • Include a robust set of capabilities that exceeds those of current record systems • Acquire a system that can be continuously updated to reflect industry leading practices • Migrate data in existing systems without losing any information • Revise existing process flows to improve efficiency and quality • Train staff with minimal interruption to existing operations

Agreement, Memorandum of Agreement, or Memorandum of Understanding, to establish and manage relationships with organizations.

HEALTH INFORMATION EXCHANGE (HIE)

The term, “Health Information Exchange”, is used either as a verb or a noun depending on the context:

As a Verb: The act of electronically sharing data amongst key stakeholders in a healthcare system, including patients, providers’ health plans, and third parties such as business associates.

As a Noun: State, federal, and private organizations that engage in electronic HIE.

HIE has moved from being periodic events – information shared at agreed-upon intervals – to being driven by “real time” data exchange protocols. Data exchanges typically use a query and response protocol (an organization electronically requests the data and the other organization sends the requested information) that allows for the sharing of health, benefits, and administrative information, including personnel records and military history records. Note that “query and response” is referred to as “subscribe and publish” in some HIE literature. DoD has a long history of using HIE to share information with the VA. Currently, the new area of focus is to be able to send and receive data with private sector partners. To accomplish this task, DoD has

joined the eHealth Exchange, an HIE that has approximately 50 other participants including VA, Social Security Administration, and Kaiser Permanente. Each eHealth Exchange participant must sign the Data Use and Reciprocal Support Agreement, which requires compliance with HIPAA Privacy, Security, and Breach Notification Rule requirements.

VIEWERS (JLV, HAIMS, VLER, BHIE, FHIE)

DoD has embarked on an ambitious project to consolidate its viewers into one because currently, DoD uses multiple mechanisms to view electronic data received from other organizations. For example, the Joint Legacy Viewer (JLV) enables DoD and VA to see data in the Service Treatment Record and records from Military Treatment Facilities (MTFs); the Health Care Artifact and Image Management System (HAIMS) provides DoD and VA healthcare clinicians with global access to radiographic images and documents generated during healthcare delivery; and the Virtual Lifetime Electronic Record (VLER) viewer allows insight into data generated by participants in the eHealth Exchange. Transitioning to a new viewer will entail interim steps, whereby capabilities from one viewer will be incorporated into another before the final transition to the Solution Agnostic Viewer.

ELECTRONIC HEALTH RECORD (EHR)

DoD has continued the process of acquiring an EHR from a private vendor by releasing a Request for Proposal. EHRs are essentially digital medical records. They may vary by the type of data they maintain – referred to in the DoD environment as domains – such as laboratory results, physician encounters, hospitalizations, and even dental

procedures. Private sector EHRs operate on proprietary platforms but usually achieve interoperability with other systems by using clinical and technical data standards produced by industry and governmental bodies, such as the Office of the National Coordinator.

i WHAT ARE REQUIREMENTS?

Functional users of emerging technologies have an integral role to play in the development of IT capabilities. As front line staff, providers and administrative personnel must communicate their needs to the technical developers of systems. For example, as DoD develops HIE, EHR, and Viewer capabilities, functional experts in the Privacy Office have provided continuous input regarding Privacy Act and HIPAA compliance system needs.

The process of developing requirements usually begins with functional subject matter experts building use cases, a high level description of a typical process – such as a Service Member visiting a provider at an MTF – and then delineating that use case into more detailed functional needs, called business or functional requirements. Business requirements can fulfill both clinical and administrative needs and describe what the system must be able to do. Information management staff will assist the functional users in formulating requirements. IT experts will then translate the business requirements into technical requirements that can be used to program executable software.

A photograph of a server room with rows of server racks. The racks are dark with glass doors, and the room has a light-colored floor and ceiling with recessed lighting.

POINT OF CONTACT

dha.ncr.pcl.mbx.

dha-privacy-office-mail@mail.mil

for questions related to HIE or emerging technologies

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on HIE.

ASD(HA) Memorandum

Recommended Best Practices for Engaging with Health Information Exchange Organizations, April 5, 2012

HIPAA Privacy Web Page

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS>

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
(currently under revision)

HIPAA Privacy Rule

45 CFR Parts 160 and 164

HIPAA Security Rule

45 CFR Parts 160, 162 & 164

DoD Health Information Security Regulation

DoD 8580.02-R, July 12, 2007
(currently under revision)

FEDERAL PRIVACY REQUIREMENTS UNDER THE PRIVACY ACT AND E-GOVERNMENT ACT

Privacy Requirements Compliance

All federal executive branch agencies, whether a covered entity (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-Government Act of 2002, and associated regulations and guidance. DoD implements the Privacy Act with DoD 5400.11-R, DoD Privacy Program.

THE PRIVACY ACT

The Privacy Act establishes safeguards and protects personally identifiable information (PII) of U.S. citizens and permanent resident aliens maintained by agencies (or by contractors on their behalf) when the information is within a Privacy Act system of records. The Privacy Act mandates that the United States Government maintain only what is needed to accomplish agency business and ensure that information is accurate, relevant, timely, and complete. The Privacy Act provides for civil and criminal penalties under certain circumstances. The Privacy Act was designed in part to embody the Fair Information Practice Principles (FIPPs) established in 1973 by the Department of Health, Education, and Welfare (predecessor to the Department of Health and Human Services [HHS]). These FIPPs promote the basic fairness of an agency collecting, using, and maintaining PII of individuals.

MAIN PRIVACY ACT REQUIREMENTS

Access and Amendment of Records – Privacy Act Request – An individual may generally be

provided access to, and a copy of, information about that person from a Privacy Act system of records upon written request. The individual may also seek amendment of information about him or herself upon showing that it is inaccurate. The DHA Privacy Office administers Privacy Act requests for DHA-managed information.

Accounting of Disclosures – Agencies who disclose PII lawfully outside the agency, except for Freedom of Information Act (FOIA) or Privacy Act requests, or for internal agency use, must be prepared to give account to the individual for disclosures made, dating back five years. The accounting must include to whom the information was disclosed and the date, nature, and purpose of the disclosure.

Computer Matching Agreements – When agencies must compare two databases for benefits determinations or cost recoupment, specific procedures must be followed, including approval by an agency Data Integrity Board and publication in the Federal Register describing the

data matching effort. Such agreements have time limits and must be re-reviewed before extensions can occur. The DHA has such an agreement with HHS Office for Civil Rights.

Government Contractors – The agency must ensure that whenever a contractor manages a system of records for the agency, that contractor is required to abide by all Privacy Act requirements as if they were an employee of the agency.

Privacy Act Statement (PAS) – When collecting PII using a form or a set of questions, a PAS must be provided. Though generally included on the face of the form, it may also be distributed on a separate sheet given with the form. Web forms must display the PAS prominently. The PAS must briefly include authority for collecting the information (usually a statute), purpose of the collection, indicate with whom shared, whether voluntary or not, and any consequences of not providing the information. Note that a form is considered voluntary unless failure to complete it violates a law or regulation. An example of an involuntary form is a required tax form.

System of Records Notices (SORNs) – SORNs must be published in the Federal Register in advance for each Privacy Act system of records. This is 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 or symbol, or other identifying particular assigned to the individual.” An agency must publish a SORN in the Federal Register identifying and describing systems maintained by that agency. This notice must specify the system owner and address, privacy data elements collected, the purpose and authority for the system, with whom the information can be lawfully shared on a routine basis outside the



THE PRIVACY ACT SETS THE STANDARD FOR SHARING PII AS INFORMED WRITTEN CONSENT

There are 12 exceptions to this requirement. Sharing without such consent may occur when sharing:

1. Occurs within the agency to accomplish an agency mission
2. Is required under FOIA
3. Outside the agency is permitted under a routine use specified by a SORN
4. To the Bureau of Census for a valid activity
5. For statistical research if transferred in a form not individually identifiable
6. To National Archives and Records Administration when historical interest warrants
7. To another U.S. or state governmental jurisdiction for a civil or criminal law enforcement activity under certain circumstances
8. Under compelling circumstances affecting the health or safety of an individual
9. To a Congressional committee for a matter within its jurisdiction
10. To the Government Accountability Office for performance of its duties
11. Pursuant to an order of a court of competent jurisdiction
12. To a consumer reporting agency under section 3711(e) of Title 31

THE FAIR INFORMATION PRACTICE PRINCIPLES INCLUDE:

These principles are foundational to the Privacy Act, and are also incorporated into many state and international privacy frameworks. Additionally, these principles are incorporated into many related laws such as the Fair Credit Reporting Act, the Video Privacy Protection Act, and the Children's Online Privacy Protection Act, to name a few.

Transparency	Agencies provide notice of systems collecting PII, and information about those systems including purposes and uses
Individual Participation	Individuals can access their own information from systems of records, and can correct inaccurate data
Purpose Specification	The agency must determine the specific purpose or purposes for which information on individuals is to be collected and used
Minimization	Agencies should only collect PII relevant and necessary to accomplish the mission, and retain only as long as necessary
Use Limitation	The information should only be used for the purposes originally identified by the system, or for any new purposes only to the extent compatible with the original purpose
Quality and Integrity of the Data	To the extent feasible, an agency must ensure that data is collected from reliable sources and is relevant, accurate, timely, and complete
Security	Agencies must protect the confidentiality, integrity, and availability of the data using appropriate security safeguards
Accountability	There must be a designated person or office for an information system or program to ensure compliance with these principles and an ability to seek redress for failures to do so

agency, and the safeguards used to protect the confidentiality of that system.

NOTE: If you deal regularly with SORNs, make sure all staff understand the specific uses and adhere to them fully.

THE E-GOVERNMENT ACT OF 2002 (INCLUDING THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT [FISMA])

In 2002, Congress passed the E-Government Act which set forth many information technology

(IT) requirements for executive agencies. The purpose of the Act is “to enhance the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer (CIO) within the Office of Management and Budget (OMB), and by establishing a broad framework of measures that require using Internet-based IT to enhance citizen access to government information and services, and for other purposes.” Within the E-Government Act are some key privacy related requirements for agencies.

MAIN E-GOVERNMENT ACT AND FISMA REQUIREMENTS

Privacy Impact Assessments (PIAs) are required for systems. Systems containing PII (especially regarding members of the public, but subsequent guidance has expanded this to PII regarding employees also) require a PIA. A PIA is a collaborative effort between the program office that operates and owns the system, the CIO's office including cyber security, and the Privacy Office, to ensure the system complies with pertinent requirements and adequately addresses any risk to privacy information.

What is a “system” for PIA purposes? A system will generally be either a major application or a general support system, as defined by OMB Circular A-130, Appendix III. A major application is one that requires special attention due to the risk and magnitude of harm from loss or unauthorized access. A general support system is an interconnected set of information resources under the same direct management control that shares common functionality and normally includes hardware, software, information, data, applications, communications, and people. In general, a system security plan is not required for minor applications because the protections associated with the larger systems generally already provide the appropriate security controls based on the general support system or major application in which they operate.

Privacy notices must be posted on agency websites and must detail:

- What information is collected
- Why the information is collected
- Intended use by the agency, including with whom it will be shared

- What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared
- Rights of the individual under the Privacy Act
- Any related information

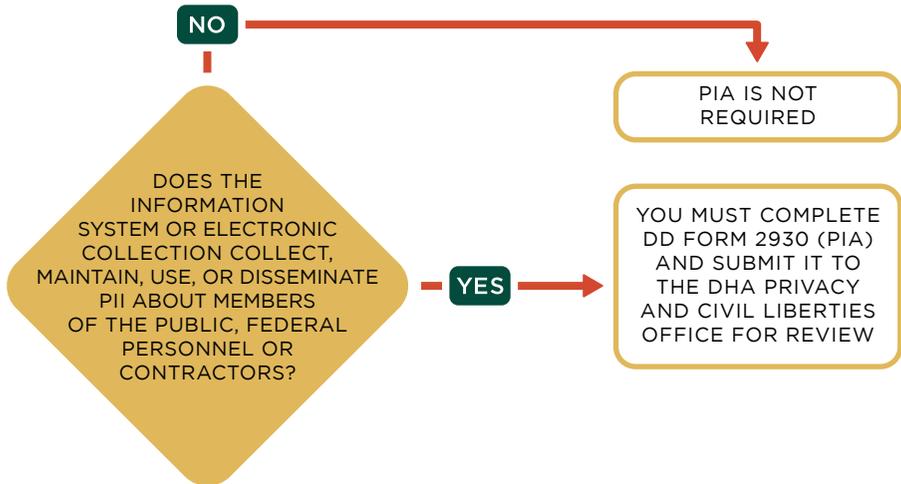
Privacy policies of agencies must be in “machine-readable” formats. The “machine-readable” formats can be automatically compared to settings on websites and receive notifications if the settings do not match.

Training in IT Security and Privacy-related topics are required through FISMA in the areas of information security and related fields based on roles. This is understood to include privacy training based on roles. The requirement is met at DHA by the workforce taking IT security awareness training, and HIPAA and Privacy Act training initially upon employment, and annually thereafter. Additional role-based training is also available, such as HIPAA Privacy Officer and HIPAA Security Officer training for those filling such roles through the MHS. Contact the DHA Privacy Office for further information.

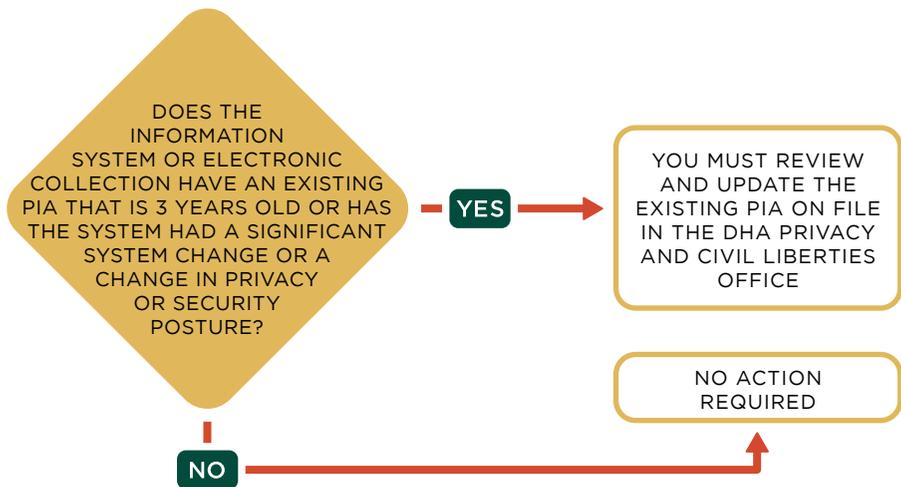
Annual reporting on compliance with Privacy Act and E-Government Act requirements.

FISMA also requires agency compliance with standardized system security requirements, and requires an annual report which goes to OMB and Congress after the end of each fiscal year. This annual FISMA Report includes a major section of security systems compliance, and one of Privacy compliance including information on the completion of SORNs and PIAs of the agency, among other data elements.

DO I NEED A PRIVACY IMPACT ASSESSMENT?



Section 208 of the E-Government Act of 2002 establishes Government-wide requirements for conducting, reviewing, and publishing PIAs.

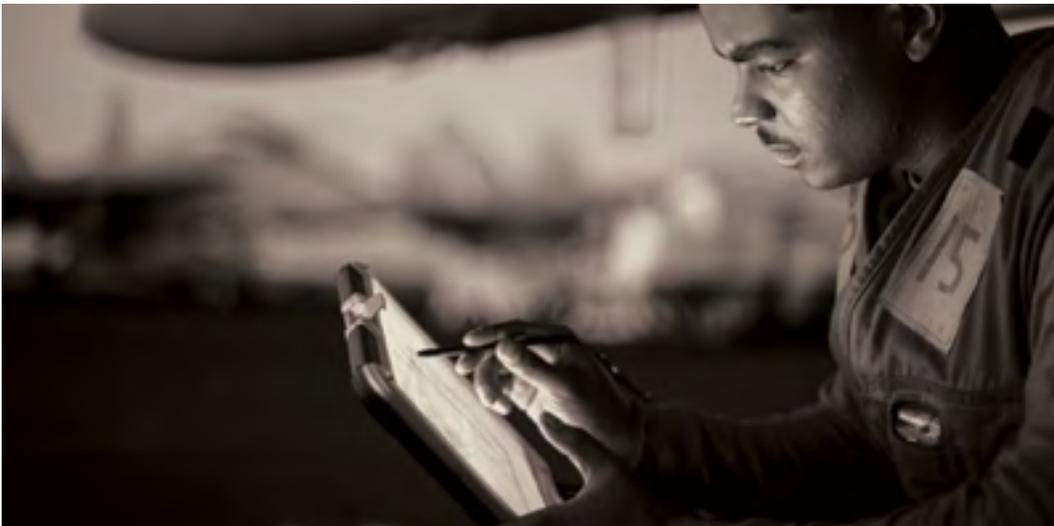


DO I NEED A SYSTEM OF RECORDS NOTICE?

If a system of records is created or maintained, a SORN must be published in the Federal Register before the system of records collects any information from or about an individual. A system of records may exist if the following questions are all answered yes:

- 1 Is information about an individual collected, maintained, or used by DoD or a contractor on DoD's behalf?
✓ Answer no if only collected to verify a person's identity and then deleted
- 2 If the answer to question 1 is yes, does the information collected include PII?
✓ Answer yes even if the individual is an employee or Service member
- 3 If the answer to question 2 is yes, is the information retrieved by the individual's unique identifier?
✓ Answer no if the system can retrieve by a unique identifier, but does not
✓ Answer no if the system only retrieves by non-unique identifiers such as a case number
✓ Answer no if the system only retrieves by a unique identifier when an individual asks for his or her own records

Note that the form of the information (paper, electronic, or combination) does not matter. For further guidance on systems of records and SORN selection, please visit the DHA Privacy and Civil Liberties Office website (<http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties>).





POINT OF CONTACT

dha.ncr.pcl.mbx.
dha-privacy-office-mail@mail.mil
for federal privacy-related questions

RESOURCES

Enclosed CD
Please see the enclosed CD for a detailed presentation on Federal Privacy.

DoD Privacy Program
DoD 5400.11-R, May 14, 2007
(currently under revision)

The Privacy Act
5 United States Code 552a, as amended

The E-Government Act of 2002
Public Law 107-347

DHA'S CIVIL LIBERTIES PROGRAM

Safeguarding Civil Liberties

Civil Liberties are liberties based on the United States Constitution, particularly the Bill of Rights (the First 10 Amendments). They include such rights as freedom of speech, religion, press, assembly; freedom from unreasonable searches and seizures; and freedom to bear arms. The 9/11 Commission Report, formally named the Final Report of the National Commission on Terrorist Attacks Upon the United States, referred to civil liberties as “precious liberties that are vital to our way of life.” The 9/11 Commission Report and subsequent legislation, identified the protection of civil liberties as a key federal priority. This was especially true due to the creation of the Information Sharing Environment, in which agencies can more proactively share information about individuals.

In 2007, Congress passed Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007 (“9/11 Commission Act”). Section 803 of the Act requires certain federal law enforcement and homeland security-related agencies, including DoD, to institute new, strong civil liberties protections. These included establishing a civil liberties program at the agency and appointing a senior official to oversee such a program, to advise on civil liberties, and to meet certain statutory requirements. Therefore, the DoD Director of Administration and Management was appointed to serve as the DoD Civil Liberties Officer (CLO), and instructed DoD components to establish component level civil liberties programs and designate a civil liberties officer to oversee compliance. On January 26, 2011, the Privacy Office’s name was changed to the TRICARE Management Activity Privacy and Civil Liberties Office. As of October 1, 2013, with the establishment of the DHA, the office

is now referred to as the DHA Privacy and Civil Liberties Office (Privacy Office).

A component Civil Liberties program has a number of primary responsibilities, which include:

- Writing policies and procedures
- Adjudicating and resolving civil liberties complaints
- Making civil liberties training available to leadership and workforce
- Analyzing draft policies and proposed actions for civil liberties implications
- Fulfilling reporting requirements to DoD and ultimately Congress
- Promoting a climate of civil liberties awareness and compliance
- Participating as a Board Member in the greater DoD Civil Liberties Board

In Administrative Instruction 64, it is DHA's policy to protect the privacy and civil liberties of DHA employees, Service members, family members, and the public with whom they come into contact, to the greatest extent possible, consistent with operational requirements. When faced with questions concerning the potential impact that DHA employees' and contractors' work may have on an individual's civil liberties, please reach out to the Privacy Office for guidance. The DHA Civil Liberties Program won awards for Outstanding Program in 2013 and 2014, and was designated Top Program for 2014 among DoD components.



CIVIL LIBERTIES BEST PRACTICES

- Do not collect information on how an individual expresses their religious beliefs or other fundamental principles
- Do not collect information on the types of organizations with which an individual affiliates

BILL OF RIGHTS

The First Ten Amendments of the U.S. Constitution, also known as the Bill of Rights, offer the following civil liberties protections:

FIRST AMENDMENT	Freedom of speech, religion, press, peaceful assembly, and the right to petition the government for a redress of grievances
SECOND AMENDMENT	Right to keep and bear arms
THIRD AMENDMENT	Right not to have soldiers quartered in any house, without the consent of the owner
FOURTH AMENDMENT	Freedom against unreasonable searches and seizures
FIFTH AMENDMENT	Right against self-incrimination and to not be deprived of life, liberty, or property, without due process
SIXTH AMENDMENT	Right to a speedy trial
SEVENTH AMENDMENT	Right to a trial by jury in cases over twenty dollars
EIGHTH AMENDMENT	Freedom from cruel and unusual punishment
NINTH AMENDMENT	Protects "non-enumerated rights", i.e. right to travel, right to a presumption of innocence
TENTH AMENDMENT	The reservation of "States rights" – This Amendment makes it explicit that the Federal Government is limited only to the powers granted in the Constitution

KEY TERMS

Chief Civil Liberties Officer – Senior Service member or civilian employee with authority to act on behalf of the Component Head and to direct the Component’s compliance with Public Law 110-53, “Implementing Recommendations of the 9/11 Commission Act” (42 U.S.C. 2000ee-1) and the DoD Civil Liberties Program.

Civil Liberties – Offer protection to individuals from improper government action and arbitrary governmental interference. They are the freedoms guaranteed by the Bill of Rights – the first 10 Amendments to the U.S. Constitution – such as freedom of speech, press, or religion, and due process of law.

Complaint – An assertion alleging a violation of privacy and/or civil liberties.

Violation of Civil Liberties – Undue government interference with the exercise of fundamental rights and freedoms protected by the U.S. Constitution.



POINT OF CONTACT

Civil_Liberties@dha.mil
for DHA civil liberties-related questions

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on the DHA’s Civil Liberties Program.

Implementing Recommendations of the 9/11 Commission Act of 2007

Public Law 110-53

DoD Civil Liberties Program

DoD Instruction 1000.29, May 17, 2012

Organizational Placement and Structure of DoD CLO Functions

DoD Directive, December 14, 2009

Protection of Civil Liberties in the DoD

DoD, Office of the Secretary of Defense, 12888-10, November 1, 2010

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
(currently under revision)

DoD Health Information Security Regulation

DoD 8580.02-R, July 12, 2007
(currently under revision)

Civil Liberties Program Case Management System

Director of Administration and Management 01, January 19, 2011

DHA Civil Liberties Program

DHA Administrative Instruction, Number 64, April 24, 2013

THE FREEDOM OF INFORMATION ACT

Access to Records through the FOIA or the Privacy Act of 1974

The Freedom of Information Act (FOIA) is a federal law enacted in 1966 that grants the public access to information possessed by government agencies. 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.

KEY TERMS

Administrative Appeal – A request to a federal agency asking that it review an initial FOIA determination at a higher administrative level.

Agency Record – The products of data compilation, regardless of physical form or characteristics, made or received by the DHA in connection with the transaction of public business and preserved primarily as evidence of the organization, policies, functions, decisions, or DHA procedures.

Backlog – The number of requests or administrative appeals which are beyond the statutory time period for a response.

Complex Request – A FOIA request that an agency anticipates will involve a voluminous amount of material to review or will be time-consuming to process.

Consultation – The procedure whereby the agency responding to a FOIA request first forwards a record to another agency for review

because the other agency has an interest in the document. Once the consulting agency finishes reviewing the record, it responds back to the forwarding agency. That agency, in turn, responds to the FOIA requester.

Expedited Processing – An agency processing a FOIA request ahead of other pending requests when a requester satisfies the requirements for expedited processing as set forth in the statute and agency regulations.

FOIA Request – A request submitted in accordance with FOIA in order to obtain previously unreleased information and documents controlled by the United States Government.

Full Denial – An agency decision not to release any records in response to a FOIA request because the records are exempt in their entirety under one or more of the FOIA exemptions.

Full Grant – An agency decision to disclose all records in full response to a FOIA request.

“Other” Response – Any response not fitting into the other categories of Full Grant, Partial Grant, or Full Denial. Examples include “no records”, “not an agency record”, or “administratively closed”, for example, because scope or fee issues were never resolved.

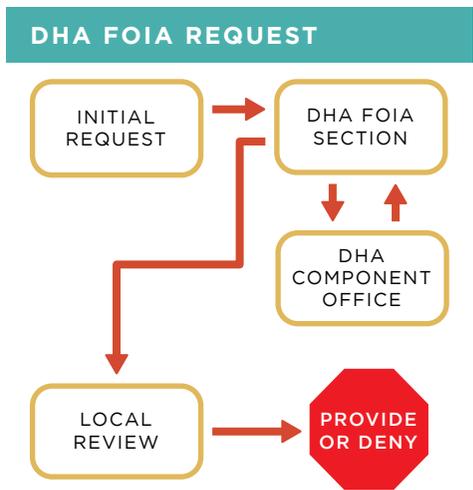
Partial Grant/Partial Denial – An agency decision in response to a FOIA request to disclose portions of the records and to withhold other portions that are exempt under FOIA, or to otherwise deny a portion of the request for a procedural reason.

Pending Request or Pending Administrative Appeal – A request or administrative appeal for which an agency has not taken final action in all respects.

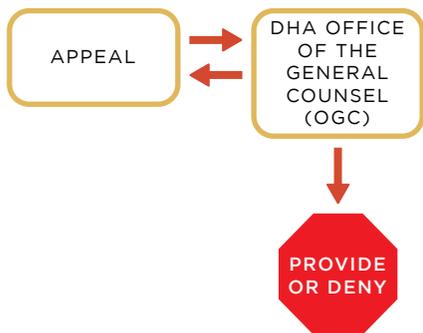
Perfected Request – A request for records which reasonably describes the records sought and is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed.

Request Type – A FOIA request from the media, commercial, or “other” use such as an individual or non-profit.

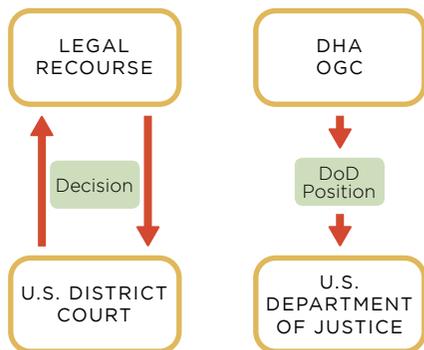
Simple Request – A FOIA request that an agency places in its fastest (non-expedited) track based on the low volume and/or simplicity of the records requested.



DHA APPEALS



LEGAL ACTION





FOIA EXEMPTIONS

FOIA restricts the release of certain documents to the public by way of the following nine exemptions:

1. Classified information that would damage national security
2. Internal personnel rules and practices
3. Information exempted from other federal statutes
4. Trade secret, privileged, or confidential commercial or personal financial data
5. Privileged inter-agency or intra-agency memorandums or letters
6. Specific sensitive personal information
7. Law enforcement records
8. Information related to government regulation of financial institutions
9. Certain geological/geographical data

In addition to the exemptions, three exclusions may restrict the release of certain records by way of the 1986 FOIA amendments:

1. Federal law enforcement agency records of ongoing investigations or proceedings
2. Records maintained by law enforcement agencies under an informant's name
3. Law enforcement records of the Federal Bureau of Investigation

ACCESS UNDER THE PRIVACY ACT OF 1974

The Privacy Act allows individuals to:

- Seek access to records retrieved by their name and personal identifier from a system of records
- Seek the amendment of any inaccurate information
- Provide written authorization for representatives to act on their behalf
- Seek records on behalf of a minor child if they are the legal guardian or parent and are determined to be acting in the minor's best interest

DHA FOIA Service Center

The DHA FOIA Service Center processes both FOIA requests and Privacy Act requests for the DHA. If a workforce member receives requests for information, please refer to the FOIA Service Center.

Requests under the FOIA and the Privacy Act need to be as specific as possible in order to identify the requested records.



POINT OF CONTACT

FOIARequests@tma.osd.mil

for FOIA-related questions or for requester status updates

RESOURCES

Enclosed CD

Please see the enclosed CD for a detailed presentation on FOIA.

Exemptions and/or the FOIA Process

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/FOIA>

FOIA Electronic Reading Room

www.tricare.mil/tma/privacy/FOIAelectric.aspx

Appeals or Complaints

<http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/FOIA/File-a-FOIA-Appeal>

White House Presidential Memorandum FOIA

www.whitehouse.gov/the_press_office/Freedom_of_Information_Act/

Executive Order 13489 – Presidential Records

<http://edocket.access.gpo.gov/2009/pdf/E9-1712.pdf>

OPEN Government Act of 2007

www.usdoj.gov/oip/amendment-s2488.pdf

DoD Privacy Program

DoD 5400.11-R, May 14, 2007
(currently under revision)

