

Health Information Privacy and Security

Training Manual

JUNE 2016



**DHA PRIVACY AND
CIVIL LIBERTIES OFFICE**
Defending Privacy



**DHA PRIVACY AND
CIVIL LIBERTIES OFFICE**
Defending Privacy

Mailing Address:

DHHQ Headquarters
7700 Arlington Boulevard
Suite 5101
Falls Church, VA 22042

Privacy Office Location:

8111 Gatehouse Road
Suite 310
Falls Church, VA 22042
703-275-6363

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. DHA achieved Full Operating Capability in October 2015, and VADM Raquel C. Bono has continued to move our agency forward. She has challenged all of us to enhance our relationship with the Services, evolve our Combat Support Agency understanding, and optimize DHA operations.

The Privacy Office seeks to accomplish the goals in our mission through numerous collaborative efforts with the Services, meaningfully underscoring the ways our privacy protection and compliance efforts support the U.S. Military mission, and aspiring toward best practices and procedures everywhere we can.

We in the Privacy Office are vigorously invested in protecting privacy and HIPAA compliance, supporting compliance in data sharing and human research protection, responding properly to FOIA requests, and promoting Civil Liberties. We have been working on building a culture of privacy protection at DHA, which I believe has become strong. One means is our outreach and training efforts, including our annual Health Information Privacy and Security Training.

It is my hope that this Training Manual will assist you with useful guidance and information to support your privacy-related activities at the DHA. Thank you for your ongoing efforts to protect our agency information, and please reach out to us whenever you wish to consult on any privacy-related matter.

With best wishes and thanks,

Linda S. Thomas

Chief, DHA Privacy and Civil Liberties Office



TABLE OF CONTENTS

Introduction	1
HIPAA Privacy	4
HIPAA Security	13
Privacy Overlays.....	19
HIPAA Transactions, Code Sets, and Identifiers	23
Data Sharing	26
Human Research Protection Program.....	31
Breach Response.....	34
Military Command Exception	42
Emerging Technology	49
Federal Privacy Requirements Under the Privacy Act and E-Government Act	56
DHA's Civil Liberties Program	65
FOIA.....	69

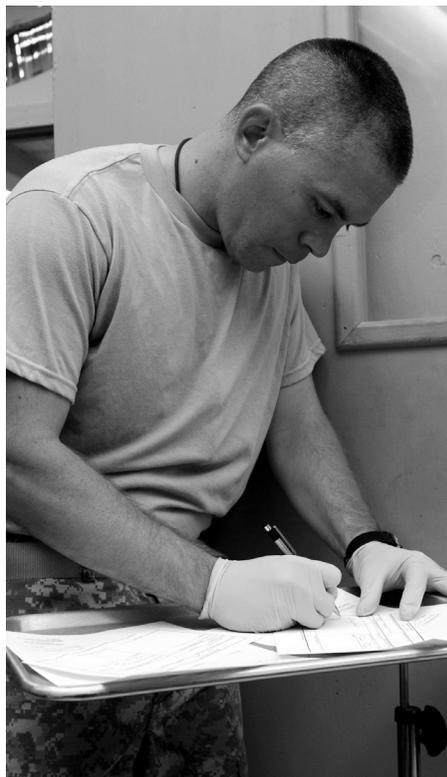


INTRODUCTION

Defense Health Agency

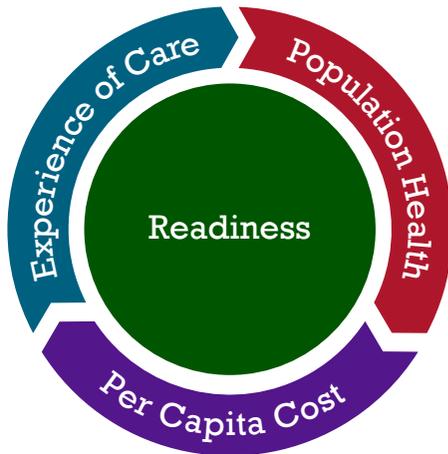
The DHA is a joint, integrated Combat Support Agency that enables the Army, Navy, and Air Force medical services to provide a medically ready force and ready medical force to Combatant Commands in both peacetime and wartime. The DHA supports the delivery of integrated, affordable, and high quality health services to Military Health System (MHS) beneficiaries and is responsible for driving greater integration of clinical and business processes across the MHS by:

- Implementing enterprise support activities with common measurement of outcomes
- Enabling rapid adoption of proven practices, helping reduce unwanted variation, and improving the coordination of care across time and treatment venues
- Exercising management responsibility for joint shared services and the TRICARE Health Plan
- Acting as the market manager for the National Capital Region (NCR) enhanced Multi-Service Market, which includes Walter Reed National Military Medical Center (WRNMMC) and Fort Belvoir Community Hospital (FBCH)



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.



Established October 2013, the DHA stemmed from a long-held conviction that military health care could be better integrated and more efficient. On its second anniversary in October 2015, the DHA achieved Full Operational Capability.

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

VADM Raquel Bono, the Director of DHA, has set DHA priorities and goals to further the Quadruple Aim key points. Her goals include enhancing DHA's relationship with

the Services, evolving and maturing Combat Support Agency understanding, and optimizing DHA operations. The DHA Privacy and Civil Liberties Office (Privacy Office) fully supports these goals, and sees its mission of privacy protection as supporting these aims. A brief overview of the Privacy Office follows.

DHA PRIVACY AND CIVIL LIBERTIES OFFICE

The DHA 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. The MHS is one of the largest integrated healthcare delivery systems in the United States, serving over 9.5 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. Included in the program overviews are references to more detailed information for each subject, along with relevant resources and contact information. New this year we have included call out boxes for greater awareness of updates in each program, as well as ways in which each topic may significantly interface with other program areas. The back pocket of this manual contains a CD with presentations from the June 7–8, 2016 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 key focus of covered entities (CEs). The HIPAA Privacy Rule was issued by the Department of Health and Human Services (HHS) in 2003, and updated in 2013, in part to address this matter. The MHS must comply with the requirements of the HIPAA Privacy Rule, both as a provider of health care and 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 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 (DoDI) 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 individuals’ 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 details 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.



PATIENT RIGHTS UNDER THE HIPAA PRIVACY RULE

HIPAA requires individuals be given certain rights and CEs are responsible for responding to individuals' requests to invoke any of these rights. When it comes to applying these rights in connection with a minor, the MHS applies the State law where the treatment is provided. See DoD 6025.18-R, paragraphs C2.4.2.1 and C8.7.3.

Under HIPAA, patient rights include:

RIGHT TO A NoPP

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

RIGHT TO REQUEST RESTRICTIONS

Individuals have a right to request that a CE restrict the use or disclosure of their PHI for TPO purposes or to persons involved in the individuals' 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

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 (PII) under the Privacy Act of 1974.

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

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 a DoD CE receiving such a request.

Under revisions to the HIPAA Privacy Rule that became effective in 2013, additional rights to restriction requests 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 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 postal mail). A CE must accommodate reasonable requests. DoD 6025.18-R, paragraph 10.2, provides additional information, including actions that may be taken by a DoD CE in connection with approving or denying such requests.

RIGHT TO INSPECT AND COPY

Individuals have a right to request to inspect and receive a copy of their PHI held by a CE in a designated record (including an electronic copy, if maintained electronically). See DoD 6025.18-R, Chapter 11. A CE

may deny such requests under certain circumstances, which include but are not limited to if the PHI:

- Involves psychotherapy notes
- Was compiled for use in, a civil, criminal, or administrative action or proceeding
- Relates to an inmate
- Pertains to research where the individual has previously agreed to not access the information while the research is in progress
- Is subject to the Privacy Act – for example, records classified in the interest of national defense or foreign policy and certain investigatory material
- Was obtained from someone other than a healthcare provider under a promise of confidentiality, and the release of the information would likely reveal the source

Under the following circumstances, a CE may deny access, but only if the individual is permitted to review the denial if:

- The access may endanger the life or safety of the individual or another person
- The PHI references another person and the access may cause substantial harm to such person



- The request is made by the individual's personal representative and the representative's receipt of the PHI may cause harm to the individual or another person

In these cases, the individual has the right to have the denial reviewed by a healthcare professional, designated by the CE, who did not participate in the original decision to deny the access to PHI.

If access to PHI is denied in whole or in part, the CE shall: 1) give the individual access to any other requested (and releasable) PHI; and/or, 2) provide a written response that contains the basis for the denial, how the individual may review the denial (if applicable), and how the individual may complain to the CE or to HHS.

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 a DoD CE receiving such a request.

RIGHT TO AN ACCOUNTING OF DISCLOSURES

Individuals have a right to know disclosures of their PHI made by a DoD CE, including disclosures by its BAs, 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 for disclosures of PHI under the following circumstances:

- 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)



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 to reflect the HIPAA Omnibus Final Rule modifications to the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule. It is important for MHS workforce members to read the NoPP and understand their rights and obligations as part of 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>.

- 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

CEs must respond within 60 days of the request regardless of whether or not the request can be fulfilled. A CE may have one 30-day extension if it provides the patient with an explanation for the extension in



writing. DoD 6025.18-R, Chapter 13, provides specific information on the process and procedures to be followed, including timelines, by a DoD CE receiving an accounting of disclosures request.

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 patient notice.

RIGHT TO FILE A COMPLAINT

Individuals have the right to file a complaint directly with a military treatment facility (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, Security, or Breach Notification Rules. Under the HIPAA Privacy Rule, a CE must provide a process for individuals to make complaints concerning the CE's policies and procedures. See DoD 6025.18-R, paragraph 14.4.

CUSTODIAL AND NONCUSTODIAL PARENTS

A minor's 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



INTERCONNECTEDNESS

Did you know the HIPAA Privacy Rule and the Privacy Act of 1974 often interact, and both must be taken into consideration in many situations? For example, a workforce member may need to demonstrate to a supervisor that he or she is physically able to perform certain job-related responsibilities. In order for a CE to disclose a workforce member's PHI to a supervisor, even just to verify the member's physical ability, it must be pursuant to a valid HIPAA authorization. Once disclosed to the supervisor, any subsequent uses or disclosures may become subject to the Privacy Act of 1974.

Additionally, requests for data such as those in a Data Sharing Agreement, take into account whether the requesting entity is permitted to receive and/or maintain PHI, and if the appropriate safeguards (as noted within the HIPAA Privacy Rule) are in place.

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.

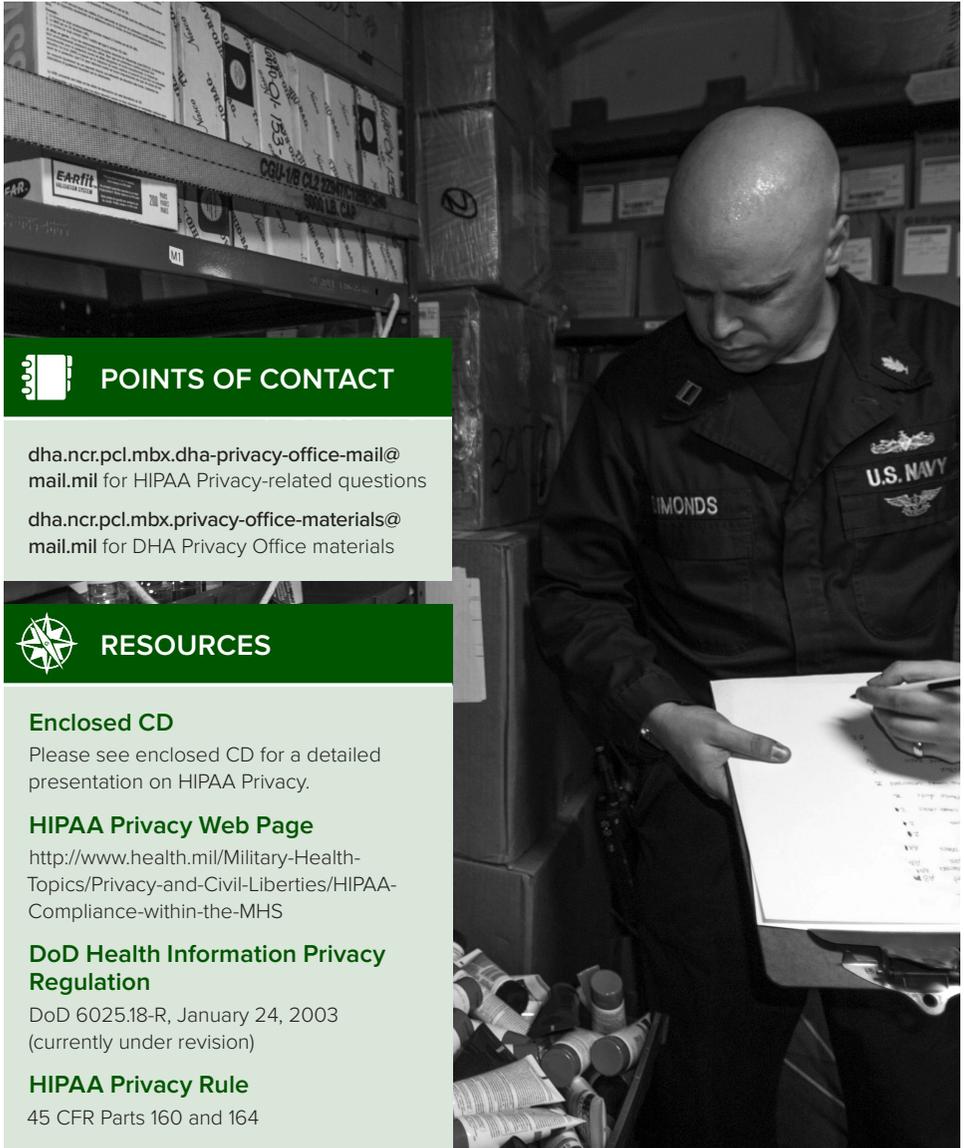


RISING STARS

DoD 6025.18-R, "DoD Health Information Privacy Regulation," which implements the HIPAA Privacy Rule within the MHS, is currently under revision. Notable changes include:

- Adoption of a new provision directing CEs that disagree with a PHI request by a military command authority to seek the advice of the cognizant HIPAA Privacy Officer or legal counsel prior to making a disclosure determination
- Incorporation of DoDI 6490.08, "Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members," which lays out the standards governing the notification of military command authorities when an Armed Forces member obtains mental health services or substance abuse education services
- Implementation of a new requirement that CEs must verify the identity and authority of any person or entity requesting PHI, if the identity or such authority is not known to the CE

Also upcoming is a HIPAA Privacy Assessment Web Tool, which is a comprehensive web-based instrument to aid MTFs in assessing their compliance with the HIPAA Privacy Rule. Upon responding to a series of HIPAA Privacy questions, the MTF will receive a customized assessment report identifying HIPAA Privacy Rule compliance opportunities and highlighting resources and best practices.



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 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)



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.

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.

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



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 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 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

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

and privacy controls identified in the Privacy Overlays.

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 DoDI 8580.02:

- 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.

DoDI 8580.02 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, policies and procedures for 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 CE's "create retrievable, exact copies of ePHI, when needed, before movement of equipment."

DoDI 8580.02 does not require DoD CE's 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," February 23, 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 personally identifiable information (PII))



INTERCONNECTEDNESS

HIPAA Security Technical Safeguards could be assessed and evaluated in relation to the NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations for additional control guidance.



RISING STARS

The Privacy Overlays released in March 2015 identify privacy and security controls that further protect and provide a repeatable, risk-based process to both select and implement security and privacy controls to protect PII and PHI.



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)

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoDI 8580.02, August 12, 2015

ASD Memorandum

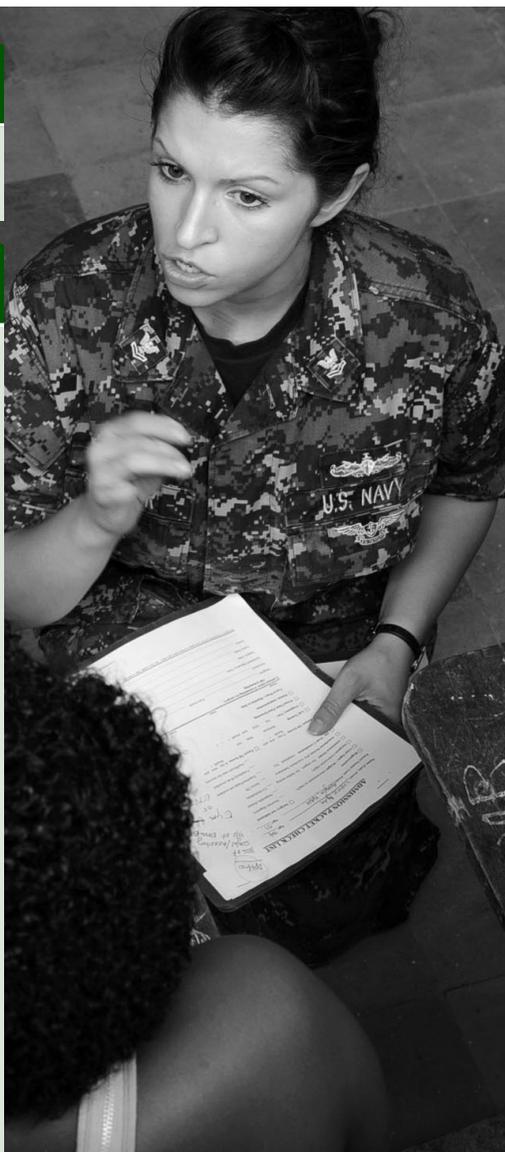
Disposition of Unclassified DoD Computer Hard Drives, June 4, 2001

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 specific guidance for electronic protected health information (ePHI) on its 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

**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)

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.

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. 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; thus 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.



INTERCONNECTEDNESS

The privacy controls within NIST SP 800-53, Revision 4, Appendix J (Privacy Control Catalog) facilitate an organization's efforts to comply with privacy requirements affecting organizational programs and/or systems that maintain PII or other activities that raise privacy risks. The Privacy Overlays also facilitate the tailoring of security control baselines to include both security AND privacy requirements (from Appendix J, page J-4).



RISING STARS

The Privacy Overlays are currently being tailored and extended further to address other "special topics" (e.g., cloud, mobile, wearables). As of March 18, 2016, DoD has released "Cloud Computing Security Requirements Guide" Version 1, Release 2 with explicit guidance to Mission Owners on the use of cloud system/application intending to store and process PII and/or PHI.

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



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

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoDI 8580.02, August 12, 2015



POINT OF CONTACT

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

HIPAA TRANSACTIONS, CODE SETS, AND IDENTIFIERS

HIPAA Compliance

The HIPAA Administrative Simplification provisions require 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 requiring a level of healthcare industry-wide commonality when it comes to electronic transmission of certain healthcare administrative information.

While the DHA Privacy and Civil Liberties Office supports MHS compliance with HIPAA Privacy and Security Rules, DHA's Business Support Directorate/Business Information Management Office facilitates MHS compliance with HIPAA TCS&I Rules. To date, HIPAA TCS&I Rules have come directly from the HIPAA legislation as well as from the Patient Protection and Affordable Care Act (also known as ACA). Mandated standards must be used when HIPAA covered entities conduct named and adopted HIPAA electronic administrative healthcare transactions that meet the purpose of the adopted standards for checking eligibility, enrollment in a health plan, referral and pre-authorization requests and claims.



WHICH HIPAA COVERED ENTITIES NEED TO COMPLY?

HIPAA TCS&I standards affect TRICARE, both as a HIPAA-covered health plan entity, and as a provider of healthcare services with person and non-person provider entities.

- Providers (e.g., military treatment facilities, civilian hospitals, civilian clinics), 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 (DMDC/DEERS), TRICARE Purchased Care Contractors)



INTERCONNECTEDNESS

For implementation of mandated HIPAA TCS&I, the DHA's Business Support Directorate/Business Information Management Office HIPAA TCS&I Program serves as the liaison between the technical system Program Offices (e.g. DHA/Health Information Technology/Solution Delivery Division) and the functional user community (e.g., Uniform Business Office) for claims processes and transactions. It also serves as a liaison for:

- Coding related to certain code sets used in HIPAA transactions
- Access to care as related to eligibility, enrollment, and referral transactions and processes
- TRICARE Private Sector Care as related to insertion of HIPAA TCS&I requirements language into TRICARE Manuals as appropriate
- Human Resources as related to implementation, availability, and use of NPI in HIPAA transactions, etc.
- The DHA HIPAA TCS&I team interacts with other Federal Agencies, healthcare industry organizations, Service Medical Department points of contact and other DHA offices

HIPAA-mandated identifiers have included the Employer Identifier, the National Provider Identifier (NPI), and the Health Plan Identifier (HPID). These identifiers are intended to be used as data within HIPAA transactions and can also be used for other non-HIPAA purposes.

HIPAA also mandates the use of certain code sets within HIPAA-adopted 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-mandated code sets can also be used for non-HIPAA purposes.



RISING STARS

The HIPAA TCS&I Program is preparing for upcoming HIPAA initiatives including Health Plan Certification of Compliance with HIPAA-mandated transaction standards and Operating Rules, Clinical Attachments, the Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase IV Operating Rules, and implementation of the next mandated version of the national standards for electronic healthcare transactions.



 **POINT OF CONTACT**

dha.ncr.bus-info-mgt.mbx.hipaacs@mail.mil for HIPAA TCS&I-related questions

 **RESOURCES**

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

DATA SHARING

Requesting Access to DHA Data

The DHA Privacy Office receives various types of data sharing requests for DHA data. 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.

KEY TERM

DHA Data – For purposes of the Data Sharing Program, DHA data is defined as personally identifiable information (PII), including protected health information (PHI), maintained on a DHA-managed system, as documented in the Defense Health Program System Inventory Reporting Tool. For example, DHA-managed systems include, but are not limited to: AHLTA, MHS Management Analysis and Reporting Tool (M2), MHS Data Repository (MDR), Theater Medical Data Store (TMDS), Composite Health Care System (CHCS), Essentris, Patient Encounter Processing and Reporting (PEPR), Defense Medical Human Resource System-internet (DMHRSi), and Pharmacy Data Transaction Service (PDTs).

DATA SHARING AGREEMENT (DSA) PROGRAM

The Privacy Office uses the DSA process to:

- Confirm that any requested use or 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
- Establish 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)

The DSAA was designed by the Privacy Office to accomplish the following objectives before a DSA is executed:

- 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

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 PII, excluding PHI
- DSA for limited data set, known as a Data Use Agreement
- DSA for PHI

RESEARCH DATA SHARING STREAMLINING INITIATIVE

An initiative is currently underway which streamlines separate and distinct reviews required by the Federal Policy for Protection of Human Subjects (also known as the “Common Rule”) and the HIPAA

Privacy Rule, so that a single board can simultaneously conduct both reviews. It further enables certain parties, subject to an agreement or policy issuance, to conduct all necessary regulatory compliance reviews that would otherwise be conducted within the DHA Privacy Office. As a result, researchers can obtain all necessary compliance reviews by the party set forth in agreement/issuance without the need for second-tier reviews within the DHA Privacy Office.

DHA PRIVACY BOARD

The DHA Privacy Board reviews research-related requests for DHA PHI and documents 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 core elements and required



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.

statements HIPAA requires researchers to include in authorizations

3. Studies that consist of research on the PHI of decedents only 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 the MHS or to contact individuals during these pre-study activities



ARE YOU READY TO SUBMIT YOUR REQUEST?

- ✓ Have you completed the most current DSAA?
- ✓ 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?



INTERCONNECTEDNESS

In the process of reviewing a DSAA prerequisite, reviews and approvals may be identified. These may include IRB approval, HRPP determination, Data Evaluation Workgroup (DEW) review, DHA Privacy Board review, Service level approval, or System Security Verification review and approval. DSAs are analyzed to ensure that Business Associates have a Business Associate Agreement (BAA) in their contract. The DSA Program supports the Program Office and Data Managers by coordinating the DSAA reviews to confirm that data requests are supported and feasible.



RISING STARS

- Multiple Service systems have transitioned to DHA and have been added to Defense Health Program System Inventory Reporting Tool (DHP SIRT)
- The DSA Annual Report will be available after the close of the fiscal year



POINTS OF CONTACT

dha.ncr.health-it.mbx.dsa-mail@mail.mil
for DSA-related questions

dha.ncr.pcl.mbx.privacyboard@mail.mil
for DHA Privacy Board, Streamlining Initiative, and MHS data expert-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)

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoDI 8580.02, August 12, 2015



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:

- 32 Code of Federal Regulations (CFR) 219, “Protection of Human Subjects” (DoD’s adoption of the “Common Rule”)
- Department of Health and Human Services (HHS) Regulation, “Protection of Human Subjects,” 45 CFR 46, the “Common Rule,” Subparts B, C and D
- 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 Protections Administrator (HPA) reviews studies that are approved by Institutional Review Boards (IRBs) with federal-wide assurance from the HHS. Non-DoD institutions must also attest to their understanding of and adherence to DoD-specific protections.



HRPP COMPLIANCE REVIEWS

HRPP compliance reviews are required for research involving human subjects and all protocols must be submitted electronically. At present, the DoD is using an e-mail-based system as we transition to a new web-based protocol management tool, Electronic IRB Second Generation 2 (EIRB2).

To submit research documents to the DHA HPA, attach them to an e-mail message addressed to dha.ncr.dha-cs-mgt-mbx.hrpp@mail.mil.

The HPA reviews include the following:

- 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 criteria are met, conducts reviews to determine whether the research is exempt from IRB review. If exempt, the HRPP Office reinforces that investigators 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 HPA 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.



INTERCONNECTEDNESS

Before a Data Sharing Agreement for research can be executed, the project must be determined to be compliant with the ethical standards for the protection of human subjects. Consequently, the DHA HRPP is tightly integrated with the DHA Data Sharing Agreement Program.



RISING STARS

The U.S. President has directed the HHS to engage all Common Rule agencies, including the DoD, in an effort to modernize the Common Rule in order to better calibrate the level of review according to risk to subjects. Further, the HHS has been directed to better accommodate advances in technology and science since the Common Rule was last updated. A new proposed Common Rule has been drafted that responds to the U.S. President's request.



POINT OF CONTACT

dha.ncr.dha-cs-mgt-mbx.hrpp@mail.mil
for HRPP-related questions



RESOURCES

HRPP Web Site

[http://health.mil/Military-Health-Topics/
Privacy-and-Civil-Liberties/Protect-Humans-
in-Research](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, November 8, 2011

BREACH RESPONSE

Prevention and Mitigation

When faced with a breach as defined by the Privacy Act of 1974 and/or the HIPAA Breach Notification Rule, equipping yourself with a clear understanding of what breaches are, why they occur, and how to prevent them is key to compliance. 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 on how to prevent breaches and how to mitigate breaches if they occur.

WHAT IS A BREACH?

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.



TOP MHS BREACH TRENDS FOR FISCAL YEAR 2015

1. Misdirected postal mail
2. Misdirected fax
3. Unauthorized access and disclosure
4. Unencrypted e-mail
5. Loss of records
6. Theft
7. Uploads to unsecured site/ shared drive



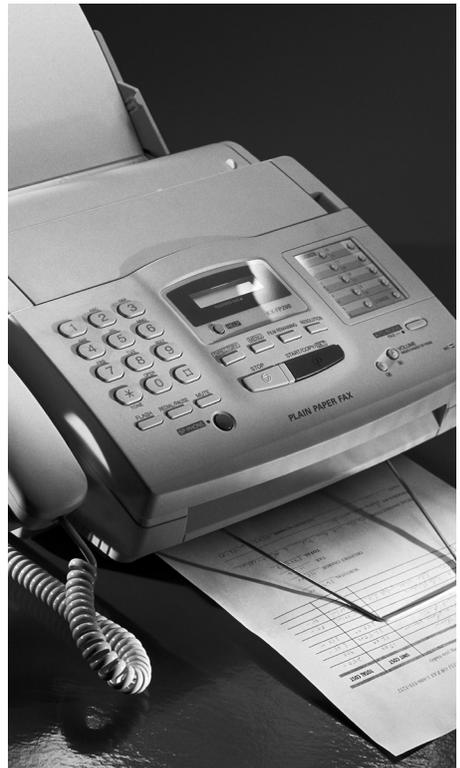
BREACH PREVENTION TIPS

- 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
- Set permissions and restrictions on electronic files and directories containing sensitive information (e.g., SharePoint, shared drives, group mailboxes, etc.)
- 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 HIPAA and Privacy Act training



BREACH PREVENTION TIPS *(continued)*

- 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 Computer Emergency Readiness Team (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.



US-CERT REPORTING REQUIREMENTS

In accordance with the Department of Homeland Security's US-CERT Federal Incident Notification Guidelines, dated January 14, 2015, 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) are not required to be reported to US-CERT.

NOTE: The above 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.

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

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



DHA ADMINISTRATIVE INSTRUCTION 71

Incident Response Team and Breach Response Requirements

Re-signed on September 15, 2015, this Administrative Instruction (AI) outlines the processes and procedures for assessing and responding to confirmed or suspected breaches occurring within DHA. Responsible individuals and supervisors should follow these guidelines when a breach or suspected breach occurs. The AI also continues the requirement to annually convene the Incident Response Team for training purposes. This year's exercise was held on March 30, 2016 at DHA.

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

BREACH POLICIES AND PROCEDURES

Policies and procedures to have an effective breach response management plan include:

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

Awareness of the applicable privacy and security policies – including updates – can be achieved when information is thoroughly disseminated to staff members through training and other forms of communication.

COMPLIANCE ENFORCEMENT

Enforcement of compliance is vital to breach prevention and should be reviewed with staff members regularly. Ensuring consequences are imposed for breaches of PII/PHI will encourage staff members 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 and security policies
- Consider stiffer penalties such as suspension, revocation of access, and/or termination
- Consistently promote awareness to prevent violations and breaches from occurring

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 HIPAA and Privacy Act 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



INTERCONNECTEDNESS

An effective breach response plan is key to an agency's preparedness; however, in order to respond to a breach correctly, a breach needs to be analyzed under Privacy Act requirements and HIPAA Breach Notification Rule requirements may also need to be considered.

In addition, while it is possible a breach may occur at any level within the MHS – from Freedom of Information Act requests to Data Sharing requests – a properly trained workforce can alleviate the impact of a breach. The synergy between an agency's workforce and breach response plan is essential in safeguarding sensitive information, preventing negative press, expensive mitigation costs, and time-consuming litigation. The failure to proactively prepare for a breach can magnify the damage caused by an incident; however, with the aid of this manual, you will become more vigilant and more prepared in preventing and responding to breaches.



RISING STARS

- In the near future, it will be a standard requirement for all DoD Components to use the universal breach reporting form, DD Form 2959
- The DPCLD is currently hosting a meeting series with major stakeholders across the DoD, including the DHA Privacy and Civil Liberties Office, on the current Breach Response Process at DoD. Expected deliverables include:
 - Recommendations on Department policy
 - Recommendations on tools
 - Recommendations on implementation of policy
- Revisions to DoD's implementation of the HIPAA Privacy Rule remain in coordination. For the first time, this DoD issuance will include HIPAA breach reporting requirements for the MHS in accordance with the HIPAA Breach Notification Rule



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 a 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>

MILITARY COMMAND EXCEPTION

Disclosing Protected Health Information 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 C7.111.2 of the DoD 6025.18-R for information on who would be considered “appropriate military command authorities.”

This exception explains when DoD providers may 1) disclose Service members’ PHI to military commanders or 2) use Service members’ PHI 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. Note that disclosures of PHI under the military command exception are permitted; they

are not required. Although non-DoD CEs are not required to abide by DoD 6025.18-R, the exception is still applicable to private hospitals and physicians as it is stated in the HIPAA Privacy Rule at 45 CFR 164.512(k)(1)(i).



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

The Department of Health and Human Services’ Office for Civil Rights (OCR) defines the term “Armed Forces personnel” within the limited scope of the HIPAA Privacy Rule’s military command exception. Specifically, OCR interprets this term to be limited only to active members of the Armed Forces.

NOTE: 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.

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 are required 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.

ACCOUNTING OF DISCLOSURES

Disclosures to military commanders must be documented for disclosure accounting purposes. See DoD 6025.18-R 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.



PHIMT ASSISTANCE

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

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 both requires and prohibits certain disclosures of mental health information to commanders. Note that DoDI 6490.08 applies 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.



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.

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 an MHS provider to a commander is a permitted "interchange...within the Armed Forces." The disclosure must separately comply with the HIPAA military command exception.

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

Under paragraph C7.111.3 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:

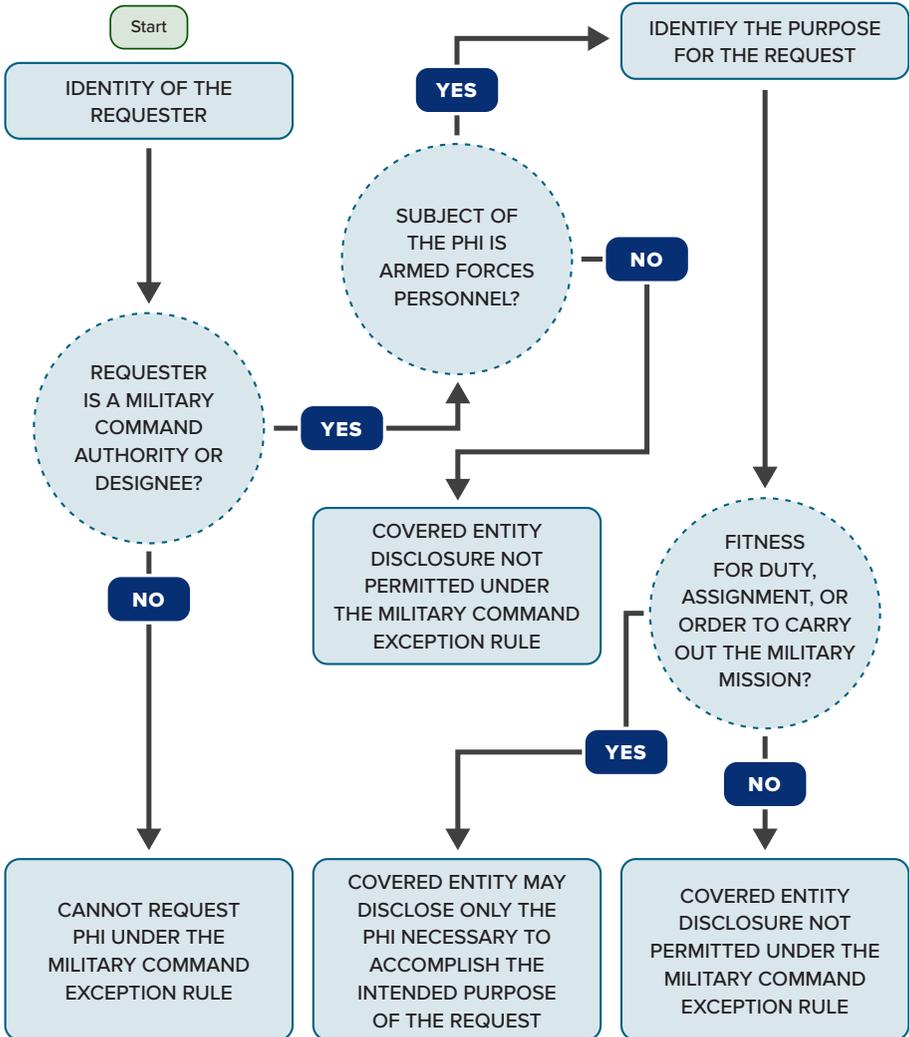
1. Determining the member’s fitness for duty, including but not limited to compliance with:
 - DoD Directive 1308.1, “DoD Physical Fitness and Body Fat Program,” June 30, 2004;
 - DoDI 1332.38, “Physical Disability Evaluation,” November 14, 1996 (incorporating Change 2, April 10, 2013); and,
 - DoDI 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

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 specific military treatment facility (MTF) personnel with authority to release PHI to commanders
2. Maintain documentation of commanders/ designees to whom Service members’ PHI may be disclosed
3. Train personnel on circumstances where PHI disclosures to military command authorities are appropriate
4. Educate personnel on the use of PHIMT to comply with disclosure accounting requirements

MILITARY COMMAND EXCEPTION DISCLOSURES





INTERCONNECTEDNESS

When it comes to uses and disclosures under the Military Command Exception, both HIPAA and Privacy Act requirements must be observed. While HIPAA applies to PHI within CEs, once the information is released it must still be protected under the Privacy Act. Failure to do so may result in a breach of PHI or personally identifiable information (PII). Therefore, it is important to educate Service members, military command authorities, and MHS providers about authorized uses and disclosures under the exception.



RISING STARS

Revisions to DoD 6025.18-R (currently in coordination) will add clarity to the Military Command Exception and its applicability within the MHS, including:

- Specifying rules governing Privacy Act applicability once PII/PHI is in a military commander's (or designee's) possession. This will ensure commanders are aware of their obligation to not further use or disclose information in an impermissible manner under existing Privacy Act policies
- Providing clarification related to Reserve or National Guard Commanders. Specifically, a Reserve or National Guard Commander "who exercises authority over an individual member...may designate...members who are medical personnel to access, receive, use, or disclose PHI of an individual under the commander's authority..."



RESOURCES

DoD Health Information Privacy Regulation

DoD 6025.18-R, January 24, 2003
(or corresponding provision in successor issuance)

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



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

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 disclosures that require consent or authorizations from

“...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**

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 (DSAs) such as a Data Use Agreement, a Memorandum of Agreement, or a Memorandum of Understanding to establish and manage relationships with organizations.

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 (JLV, HAIMS, BHIE, VLER)	<ul style="list-style-type: none"> • Consolidate current viewers into one MHS-wide viewer • Improve capability to see images • Maintain the capabilities that exist in the current viewers, at a minimum
Electronic Health Record	<ul style="list-style-type: none"> • Include a robust set of capabilities that exceeds those of current record systems • Implement 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



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 a military treatment facility (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.

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, BHIE, VLER)

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. The following are examples of those mechanisms:

- Joint Legacy Viewer (JLV) enables DoD and VA to see data in the Service Treatment Record and records from MTFs
- 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

- Bi-Directional Health Information Exchange (BHIE) allows DoD and VA providers to view inpatient and outpatient clinical data on a shared patient population
- 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 consolidated viewer which is currently being referred to as the Health Information Portal (HIP).

ELECTRONIC HEALTH RECORD (EHR)

DoD has started the process of implementing the EHR acquired from a private vendor with Initial Operating Capability Go Live scheduled for the fourth quarter of 2016. 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.

INTERCONNECTEDNESS

With the rise of HIEs, the need exists to extend data protections beyond organizations covered by the Privacy Act (federal organizations) and HIPAA (providers and health plans) because health data can now be easily shared with other entities that use it to make key decisions. The MHS supports the basic concept (initially defined in the Fair Information Practice Principles that served as the foundation for the Privacy Act and HIPAA) that individuals should have the right to participate in deciding how their data can be used and disclosed. The MHS uses many mechanisms to control not only the initial use and disclosure of data but downstream uses as well. By changing its internal policies through DoD Instructions, Administrative Instructions and other publications, the MHS has embarked on a process to align its policies and procedures to emerging data protection requirements. MHS is also upgrading its legacy systems to meet new privacy requirements and the new EHR will implement options that exceed current privacy capabilities. The MHS is a signatory to the Data Use and Reciprocal Support Agreement, which safeguards the data we share with other organizations in the eHealth Exchange, and uses DSAs to control data shared with contractors.



RISING STARS

Computable Privacy...Rise of the Machines

For the electronic capture and transmission of health information to gain and maintain widespread acceptance, patients need to trust that their information will be shared in accordance with their wishes. However, industry standards do not currently exist to communicate patient choice in such a way that the patient's selection persists as data is transmitted from organization to organization, or even internally. To solve this issue, a new capability called “computable privacy” is being developed. To accomplish computable privacy:

- Data must be machine readable
- Data elements must use standard formats
- Key definitions (e.g., “sensitive”) must be standardized using a data dictionary
- Privacy designations must persist
- Data must be transmissible among internal and external information systems and the Internet of Things (wearables, patient mobile devices, provider medical devices, infrastructure, etc.)

Computable privacy would integrate privacy protections into software design at three levels:

- First, software would incorporate HIPAA permitted uses and disclosures as background default rules, to be implemented when no patient choice is recorded



RISING STARS *(continued)*

- Second, software would solicit the patient's “basic choice” on data sharing outside the covered entity
- Finally, computable privacy would incorporate a patient's more granular choices, enabling a patient to depart from the basic opt in or opt out choice in specific situations





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

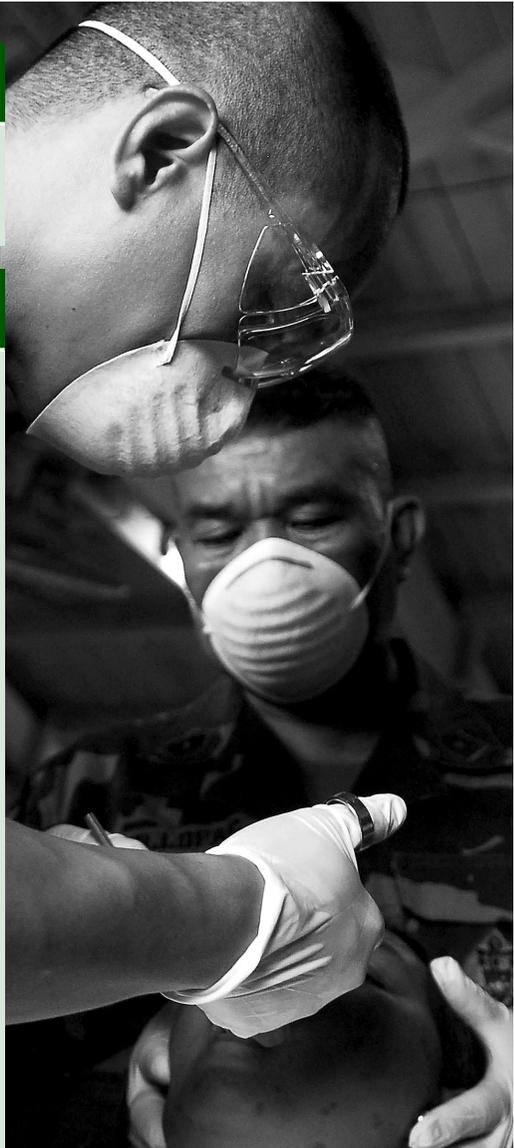
45 CFR Parts 160 and 164

HIPAA Security Rule

45 CFR Parts 160, 162 & 164

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoDI 8580.02, August 12, 2015



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 (Privacy Act) and the E-Government Act of 2002, as well as other 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 the 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 front 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 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.



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

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 be either a major application or a general support system, as defined by OMB Circular A-130, Appendix III. (OMB is revising Circular A-130 to be more efficient in today's privacy and security environment.) 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 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 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?

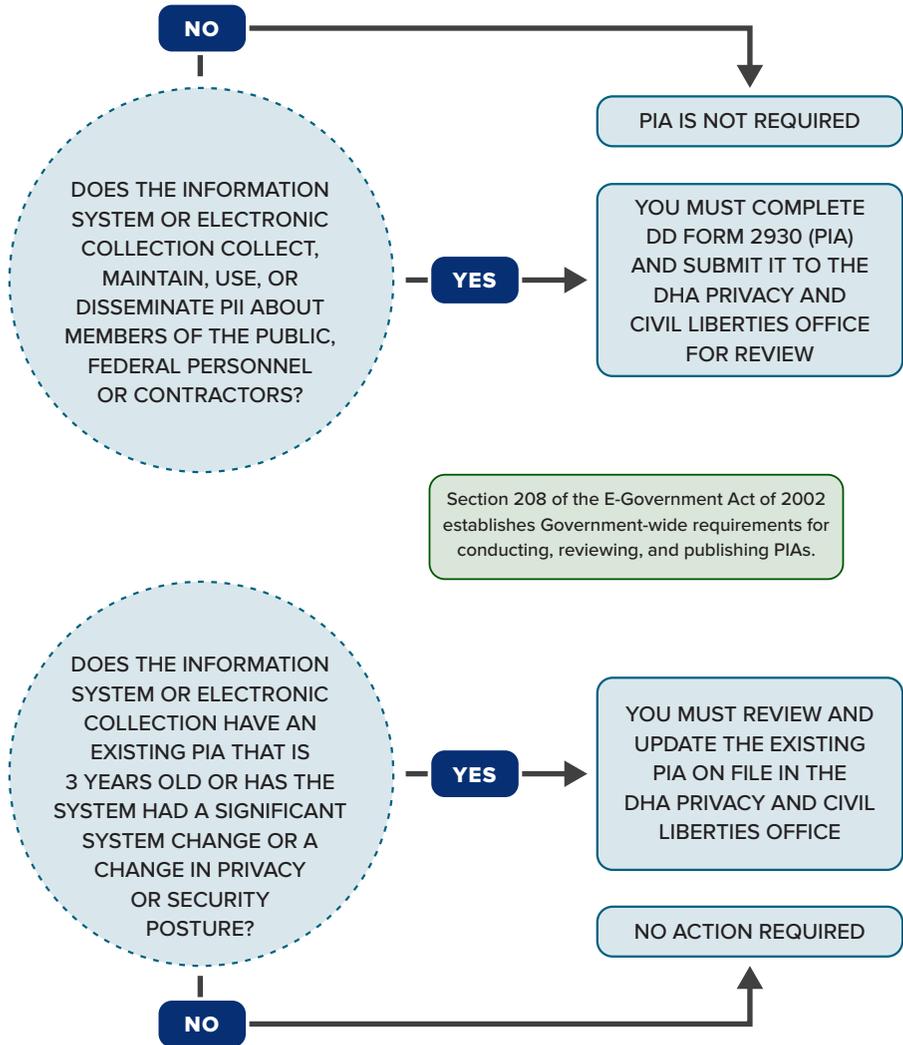
✓ Answer no if only collected to verify a person's identity and then deleted |
| 2 | If the answer to question 1 is yes, does the information collected include PII?

✓ 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>).

DO I NEED A PRIVACY IMPACT ASSESSMENT?





INTERCONNECTEDNESS

Federal Privacy requirements may arise in many situations, such as:

- When conducting a survey
- When posting information online
- When contracting for services
- When giving training or demos

Consult the DHA Privacy Office if you have questions!



RISING STARS

The OMB is revising Circular A-130: Managing Information as a Strategic Resource, incorporating “new statutory requirements and enhanced technological capabilities, as well as addressing current and evolving technical and personnel security threats.” This revision also integrates the Senior Agency Official for Privacy (SAOP) into the risk management framework and elevates the role and status of the SAOP as an equal partner to his or her security counterparts.



POINT OF CONTACT

dha.ncr.pcl.mbx.privacyactmail@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 found in the United States Constitution, particularly the Bill of Rights (the first 10 Amendments). They include rights such 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 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 it, counsel, advise on civil liberties, and 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 DHA, the office is now referred to as the DHA Privacy and Civil Liberties Office (Privacy Office). The DHA Privacy Office Chief has been designated by the DHA Director as the DHA Civil Liberties Officer.

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

- Writing policies and procedures
- Adjudicating and resolving civil liberties complaint
- 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 which 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 has won awards for its Outstanding Program in 2013, 2014, and 2015 and was designated the Top Program for 2014 and 2015 among DoD components.

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 government 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, 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.



CIVIL LIBERTIES TODAY

Civil liberties are defined as much by common law as they are by the original Bill of Rights and subsequent legislation. However, the body of law is constantly evolving. Currently, the Supreme Court is deciding on the case *Hefernan v. City of Paterson*.

This case will determine whether retaliation against an employee, because they believed an individual was exercising the First Amendment, is in any way directly detrimental to one’s employer.

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 bear arms
Third Amendment	Right not to have soldiers quartered in private residences 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



INTERCONNECTEDNESS

Civil liberties sometimes intersect with Equal Employment Opportunity and Human Resource matters. At times, a civil liberties issue will overlap with other such offices.



RISING STARS

Privacy and (International) Civil Liberties

International corporations are often storing data in servers located in other countries. This raises both privacy and Fourth Amendment concerns because many foreign jurisdictions in the western world now have rough equivalents in their jurisprudence. This is and will continue to be the subject of litigation.



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 2003
(currently under revision)

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoDI 8580.02, August 12, 2015

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 (currently under revision)



POINT OF CONTACT

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

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.

Perfect 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.



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

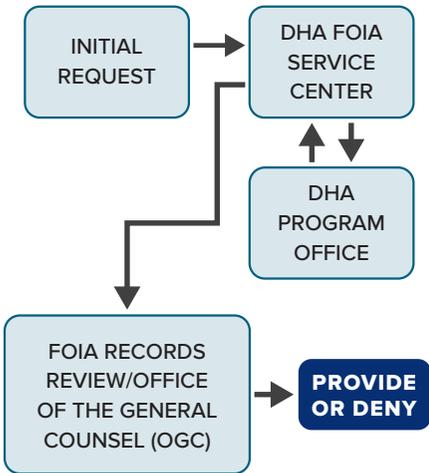
In addition to the exemptions, three exclusions may restrict the release of certain records by way of the 1986 FOIA amendments:

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

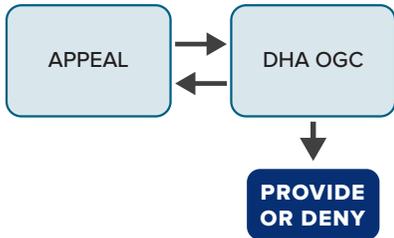
Request Type – A FOIA request from the media, commercial, or “other” use such as an individual or non-profit.

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.

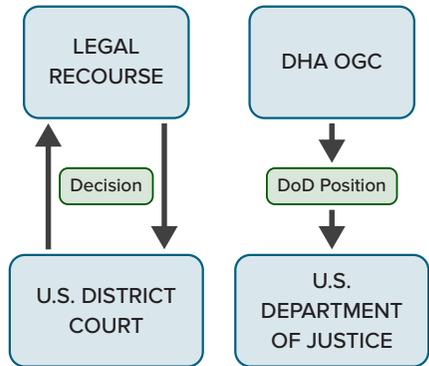
DHA FOIA REQUEST



DHA APPEALS



LEGAL ACTION



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, 703-275-6363 or dha.ncr.pcl.mbx.foia-requests@mail.mil.

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



INTERCONNECTEDNESS

The FOIA Service Center processes data requests which often require the removal of protected health information (PHI)/personally identifiable information (PII) in review. In responding to these type of requests and Privacy Act requests, HIPAA, FOIA and privacy regulations and statutes all meet and interact. For example, with FOIA requests containing PHI/PII data, we apply the usual FOIA exemptions AND mask PHI via the "rule of three," as referred to in DoD 6025.18-R and DoD Manual 6025.13, thereby de-identifying statistical data and protecting the personal privacy of patients.



RISING STARS

As DHA transitioned to a standalone agency, its FOIA policies and procedures had to be reviewed and integrated with broader DoD FOIA regulations. This process has been completed and is awaiting approval.



RESOURCES

Enclosed CD

Please see 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

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

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)



POINT OF CONTACT

dha.ncr.pcl.mbx.foia-requests@mail.mil
for FOIA-related questions or for requester status updates

