

MAY 2014

DHA PRIVACY & CIVIL LIBERTIES OFFICE



# Health Information Privacy & Security Training Manual





# 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.

The DHA Privacy Office fully supports this endeavor by ensuring vigilance in the protection of information privacy and promoting related compliance across the organization. Key elements of our work include fostering and maintaining compliance with the Privacy Act, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security, and Civil Liberties regulations, as well as responding to Freedom of Information Act requests and managing Data Sharing and Human Research Protection processes.

While the DHA Privacy Office holds responsibility for these charges, collaboration from the entire DHA workforce is required to accomplish the mission. Your support has helped the DHA get off to a tremendous start in its progress with these programs, and I thank you personally for your diligence and attentiveness to privacy protection.

We have an important calling to honor the dignity and welfare of each individual beneficiary and employee by defending their personal information, upholding civil liberties, and complying with such program requirements on their behalf. We must work together to ensure that we bear that mission in mind each and every day.

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

With best wishes and thanks,  
Chief, DHA Privacy and Civil Liberties Office



## Table of Contents

Overview .....	4
HIPAA Privacy .....	5
HIPAA Security .....	11
Privacy Overlay .....	16
HIPAA Transactions, Code Sets, and Identifiers.....	19
Data Sharing .....	21
Human Research Protection Program .....	25
Breaches and Complaints .....	27
HIPAA Audits.....	33
Military Command Exception .....	35
Health Information Exchange.....	40
Federal Privacy Requirements .....	46
Civil Liberties .....	53
Freedom of Information Act.....	56

# Overview

## Health Information Privacy & Security Training

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

- Ensuring DHA policies and business practices comply with federal laws, DoD regulations, and guidelines governing the privacy and security of PII/PHI, and in the development and of DoD HIPAA regulations, instructions, policies, and procedures
- Managing and evaluating potential risks and threats to the privacy and security of MHS health data by performing critical reviews through:
  - Evaluation of the privacy and security posture of the DHA by conducting the HIPAA required Security Risk Assessment annually
  - Performance of Compliance Risk Assessments throughout the DHA to evaluate Privacy and HIPAA compliance
  - Establishment of organization performance metrics to identify and measure potential compliance risks
  - Robust Data Sharing and Human Research Protection Programs
- Engaging DHA stakeholders, including employees and contractors, by developing and delivering education and awareness materials and ongoing workforce Privacy and HIPAA training
- Fully implementing applicable provisions of the Privacy Act, the E-Government Act, the Freedom of Information Act, and the 9/11 Commission Act of 2007, which required the establishment of a Civil Liberties program

We also provide dedicated assistance to the Director, DHA in responding to inquiries from Congress, the Office of Management and Budget, the Department of Health and Human Services, and the Department of Veterans Affairs, as well as other federal agencies and DoD components, on matters related to privacy and HIPAA.

This training guide 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 privacy and HIPAA world. Contained in the program overviews are references to more detailed information for each subject, along with relevant resources and contact information.

# HIPAA Privacy

## Complying with the HIPAA Privacy Rule

In today's world, safeguarding the privacy and security of health information is a major concern. The HIPAA Privacy and Security Rules were enacted, in part, to address this concern. The MHS must comply with the requirements of HIPAA, both as a provider of health care through Military Treatment Facilities (MTF) and as the TRICARE health plan through contracted network health care services. To implement the HIPAA Rules, DoD issued privacy and security standards within all DoD components required to comply with HIPAA. The HIPAA Privacy Rule focuses on permitted and required uses and disclosures of protected health information (PHI) as well as individual rights with respect to the PHI created or received by those regulated by HIPAA, known as covered entities (CEs), including the MHS.

### KEY TERMS

#### **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: health care plans, health care clearinghouses, and certain health care providers. The law is implemented by the Department of Health and Human Services (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.

**Covered Entity (CE)** – A health plan, a health care clearinghouse, or a health care provider that conducts one or more covered transactions in electronic form.

#### **Protected Health Information (PHI)** –

Individually identifiable health information created or received by a CE that relates to the past, present, or future physical or mental health of an individual and is transmitted or maintained in electronic, paper, or any other form. It excludes health information in employment records held by a CE in its role as employer. PHI does not include health information of persons deceased more than 50 years.

**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.

**Business Associate Agreement (BAA)** – A legal agreement between a CE and its BA that outlines responsibilities and obligations for compliance with HIPAA and the handling of PHI.

**Notice of Privacy Practices (NoPP)** – Document generated by a CE that describes how an individual's PHI may be used/disclosed, outlines individual privacy rights, describes CE obligations under the HIPAA Privacy Rule, and outlines the process for filing a complaint.

**Organized Health Care Arrangement (OHCA)** – Legally separate CEs under common ownership or control. OHCA members may exchange PHI with each other for treatment, payment, and health care operations (TPO) purposes, have a joint NoPP, and share a common BA.

- The MHS is a CE under HIPAA and includes all DoD health plans and all DoD health care providers
- The MHS is part of an OHCA that includes certain elements of the U.S. Coast Guard

### **The Health Information Technology for Economic and Clinical Health (HITECH)**

**Act** – The HITECH Act required major changes in the HIPAA Privacy, Security, and Enforcement Rules and established a new Breach Notification Rule. These changes were implemented by HHS through the HIPAA Omnibus Final Rule. The Act contains incentives related to health care information technology (e.g., creation of a national health care infrastructure) and to accelerate the adoption of electronic health record (EHR) systems among providers. The Act advocates the exchange of electronic PHI, while widening the scope of privacy and security protections available under HIPAA. It also increases the potential legal liability for HIPAA Privacy and Security Rule non-compliance and provides for more enforcement.

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

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

**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 health care provider for treatment purposes
- Disclosures to individuals or pursuant to individual's authorization
- Disclosures to HHS for HIPAA compliance purposes
- Uses or disclosures required by law

## **PATIENT RIGHTS UNDER THE HIPAA PRIVACY RULE**

HIPAA requires individuals be given certain rights, and the CE is responsible for responding to an individual's request to invoke any of these rights. These rights are listed below:

### **RIGHT TO A NoPP**

Individuals have a right to be notified how their PHI may be used and/or disclosed by the CE. Individuals must also be notified of their rights and the CE's legal responsibilities with respect to their PHI.

### **RIGHT TO INSPECT AND COPY**

Individuals have a right to inspect and request a copy of their medical or billing records (including an electronic copy, if maintained electronically). A CE must respond within 30 days after the receipt of a request, but, with written explanation, can

obtain an additional 30 days and must provide a date certain for production. Under certain circumstances, a CE may deny such requests, in whole or in part, but must provide a written explanation of the denial, and in some cases, an opportunity to have the denial reviewed.

### **RIGHT TO FILE A COMPLAINT**

Individuals have the right to file a complaint directly with an MTF HIPAA Privacy Officer, the DHA Privacy Office, and/or the HHS Office for Civil Rights if they feel a CE has violated an individual's health information privacy rights or committed a violation of the HIPAA Privacy or Security Rule provisions. A CE must provide a process for individuals to make complaints concerning the CE's policies and procedures under the HIPAA Privacy Rule.

### **RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS**

Individuals have a right to request their PHI be communicated in a certain way or at a certain location (e.g., only at home or only by mail). A CE must accommodate reasonable requests.

### **RIGHT TO REQUEST RESTRICTIONS**

Individuals have a right to request a CE restrict the use or disclosure of their PHI for TPO purposes or to persons involved in the individual's care or health care payment. A CE is not required to agree to a request unless the disclosure is to a health plan and is not otherwise required by law and the purpose of the disclosure is for payment or health care operations related to a service or product for which the individual has paid out of pocket in full. A CE may break an agreed-upon restriction if the PHI is needed for emergency treatment or if the CE informs the individual in writing. Acceptance, denial, and/or termination of a restriction must be documented by the CE.

### **RIGHT TO AN ACCOUNTING OF DISCLOSURES**

Individuals have a right to know who has received their PHI during a specific time period - up to six years prior to the date of the request - for disclosures other than:

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

CEs/MTFs must respond within 60 days of the request. A CE/MTF may extend up to 30 days, to a date certain, and must provide the patient with an explanation for the extension in writing. These response timelines do not apply if temporary suspension of the individual's right is justifiably directed by the agency receiving disclosures under the health oversight or law enforcement exceptions, and it is documented.

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



## RIGHT TO REQUEST AN AMENDMENT

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

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

If the request is denied, the CE must provide a written statement to the individual and explain their right to file a written statement of disagreement.



### *NEW MHS NoPP*

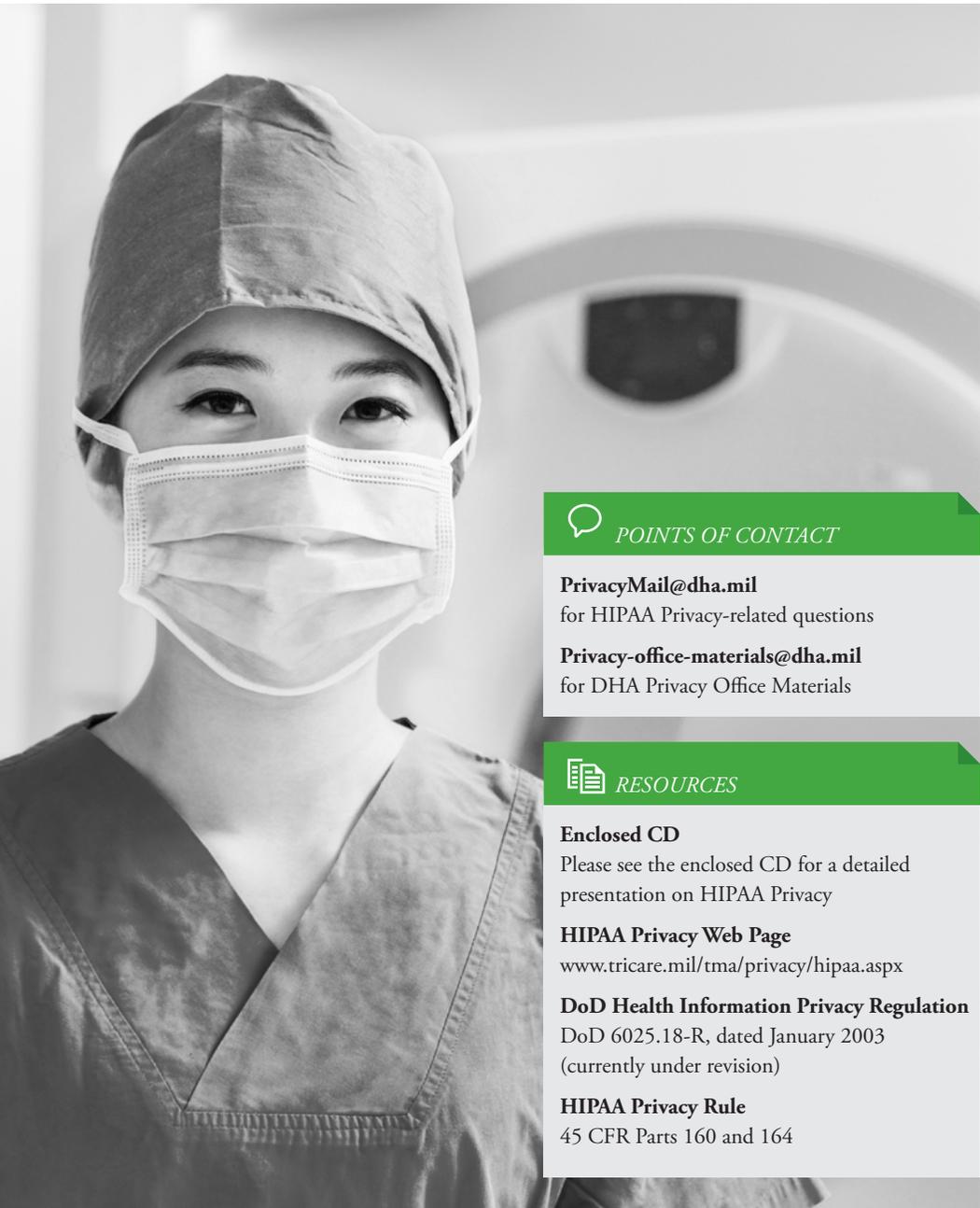
The new MHS NoPP was issued by the DHA Privacy Office on October 1, 2013. The revisions not only enhance clarity and readability, but also reflect the HIPAA Omnibus Final Rule modifications to the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule. It is important for beneficiaries and MHS workforce members to read the revised NoPP and understand their rights and our obligations as the MHS. The new 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 see: [www.tricare.mil/tma/privacy/hipaa-nopp.aspx](http://www.tricare.mil/tma/privacy/hipaa-nopp.aspx).

## CUSTODIAL AND NONCUSTODIAL PARENTS AND SPONSORS

The below table for Custodial and Noncustodial Parents and Sponsors helps determine whether an individual has a right to perform specific actions in regards to a minor's health care information and/or care. Specifically, it provides guidance on whether a custodial parent (a noncustodial parent or sponsor) or non-parent may:

- Access the Defense Enrollment and Eligibility Reporting System (DEERS) on behalf of the minor
- Access the minor's medical records, or
- Schedule the minor's medical appointments

RELATIONSHIP TO MINOR	ACCESS TO DEERS	ACCESS TO MINOR'S MEDICAL RECORDS	SCHEDULE MINOR'S MEDICAL APPOINTMENTS
Custodial Parent (TRICARE beneficiary)	Yes	Yes	Yes
Custodial Parent (non-TRICARE beneficiary)	No	Yes	Yes
Noncustodial Parent (TRICARE beneficiary)	Yes	Yes	Yes
Noncustodial Parent (non-TRICARE beneficiary)	No	Yes	Yes
Sponsor (parent)	Yes	Yes	Yes
Sponsor (non-parent)	Yes	No	No



### *POINTS OF CONTACT*

**PrivacyMail@dha.mil**

for HIPAA Privacy-related questions

**Privacy-office-materials@dha.mil**

for DHA Privacy Office Materials



### *RESOURCES*

**Enclosed CD**

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

**HIPAA Privacy Web Page**

[www.tricare.mil/tma/privacy/hipaa.aspx](http://www.tricare.mil/tma/privacy/hipaa.aspx)

**DoD Health Information Privacy Regulation**

DoD 6025.18-R, dated January 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)<sup>1</sup> 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'S COVERED?

HIPAA COVERED ENTITIES	EXAMPLES IN THE DOD
Health care 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
Health care clearinghouses	Companies that perform electronic billing on behalf of military treatment facilities
Business associates	Health care services support contractors and other contractors that provide services that require access to PHI

<sup>1</sup> ePHI is PHI in electronic form that is transmitted or maintained by electronic media. Medical 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 covered entities (CE) and business associates (BA) 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, a Privacy Overlay is being developed to identify minimum protections for ePHI. This Privacy Overlay links 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.<sup>2</sup>

As organizations conduct HIPAA risk assessments, they may find that more stringent controls are appropriate than those that have been identified in the Privacy Overlay. Nothing in the Privacy Overlay 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 and privacy controls identified in the Privacy Overlay.



### 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 impact and risk of potential risks to the confidentiality, integrity, and availability of ePHI
- ✓ Assess existing security measures
- ✓ Periodically review the risk analysis and update findings

<sup>2</sup> For additional information on the Privacy Overlay, refer to the Privacy Overlay section of this training manual.

## THE HIPAA SECURITY RULE SAFEGUARDS

### ADMINISTRATIVE SAFEGUARDS

are designed to protect ePHI and to manage the conduct of the DoD CE's workforce using ePHI in the performance of their jobs. There are nine administrative safeguards identified in DoD 8580.02-R, which is currently in coordination for re-issuance as a revised DoD Instruction.

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

The Security Management Process is a crucial standard in 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 and the Minimum Necessary Standard.

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

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

### PHYSICAL SAFEGUARDS

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

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

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

The Maintenance Records specification requires the DoD CE to keep records for 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, the DoD CE 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 time of final disposal or transfer to another person or entity.

### TECHNICAL SAFEGUARDS

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

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

Access Controls carry out the implementation of the Information Access Management standard which set the rules about 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 the DoD CE “create retrievable, exact copies of ePHI, when needed, before movement of equipment.”

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



#### *STOP AND THINK SECURITY TIPS*

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



## POINT OF CONTACT

**HIPAASecurity@dha.mil**  
for HIPAA Security-related questions



## RESOURCES

### **Enclosed CD**

Please see the enclosed CD for a detailed presentation on HIPAA Security, as well as reference material on the safeguards and implementation specifications

### **HIPAA Security Web Page**

[www.tricare.mil/tma/privacy/hipaa-securityrule.aspx](http://www.tricare.mil/tma/privacy/hipaa-securityrule.aspx)

### **HIPAA Security Rule**

45 CFR Parts 160, 162 & 164

### **DoD Health Information Privacy Regulation**

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

### **DoD Health Information Security Regulation**

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

### **ASD Memorandum**

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

### **ASD for Health Affairs Memorandum**

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



# Privacy Overlay

## Integrating Security Standards

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

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

Once completed, the Privacy Overlay will serve as 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 controls. The proposed Privacy Overlay will be used as a tool by information systems security engineers, authorizing officials, privacy officials, and others to select appropriate protections for differing privacy information types, including ePHI.

Noticeably included within this new tool will be the feature that allows privacy officials and information assurance experts the ability to align, in real-time, any existing privacy/security requirements applicable to a specific computing system containing ePHI. The use of the Privacy Overlay alongside NIST security control baselines will allow security and privacy controls to be customizable and implemented as part of an organization-wide process that manages information security and overall privacy risk.

The Privacy Overlay applies to systems and the organizations in which they reside that maintain, collect, use, or disseminate information systems that handle personally identifiable information (PII), including ePHI. This type of privacy-centered overlay will support system owners, program managers, developers, privacy programs, and those that maintain information systems by identifying security and privacy controls and requirements, both statutory and regulatory. It will also serve as a tool to develop guidance and privacy best practices.



## HOW DOES IT WORK?

Not all PII must be protected equally. NIST Special Publication (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 the PII in the system – low, moderate, or high – the methodology indicates the potential harm that could result if PII were 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 sound



### *PRIVACY OVERLAY FRAMEWORK*

- NIST SP 800-53, Revision 4, Recommended Security Controls for Federal Information Systems and Organizations, May 1, 2010
- NIST SP 800-122, Guide to Protecting the Confidentiality of PII, April 2010
- Committee on National Security Systems Instruction (CNSSI) No. 1253, Version 2, March 15, 2012

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.

Since 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 Overlay distinguishes 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). Because all PHI is PII, the laws, regulations, and other standards for safeguarding PII still apply. Therefore, the organization must follow the guidance contained in the Privacy Overlay to determine the PII confidentiality impact level of the information it owns and/or manages and apply the appropriate subpart of this Privacy Overlay. After determining the PII confidentiality impact level, the organization must also consider the guidance for PHI within the Overlay.



## POINT OF CONTACT

**HIPAASecurity@dha.mil**  
for Privacy Overlay-related questions



## RESOURCES

### **Categorization and Control Selection for National Security Systems**

CNSSI No. 1253, Version 2, March 15, 2012

### **Guide to Protecting the Confidentiality of PII**

NIST SP 800-122, April 2010

### **Recommended Security Controls for Federal Information Systems and Organizations,**

NIST SP 800-53 rev 4, May 1, 2010

### **Cybersecurity**

DoD Instruction (DoDI) 8500.01 (currently under revision)

### **Risk Management Framework for DoD Information technology**

DoDI 8510.01 (currently under revision)

### **Security of Individually Identifiable health Information in DoD Health Care Programs**

DoDI 8580.02 (currently under revision)

# HIPAA Transactions, Code Sets, and Identifiers

## HIPAA Compliance

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

While the DHA Privacy Office supports MHS compliance with HIPAA and other federal privacy and security laws, DHA's Information Management Division Branch oversees compliance with HIPAA TCS&I regulations and HIPAA Certificates of Creditable Coverage for portability. Regulations for HIPAA TCS&I mandate the electronic standards that must be used when conducting named and adopted administrative health care transactions such as enrollment in a health plan, eligibility checking, referrals, and claims processing. HIPAA-mandated identifiers include the Employer Identifier, the National Provider Identifier, and the upcoming Health Plan Identifier. These identifiers are used within HIPAA transactions to identify employers, providers, and health plans.

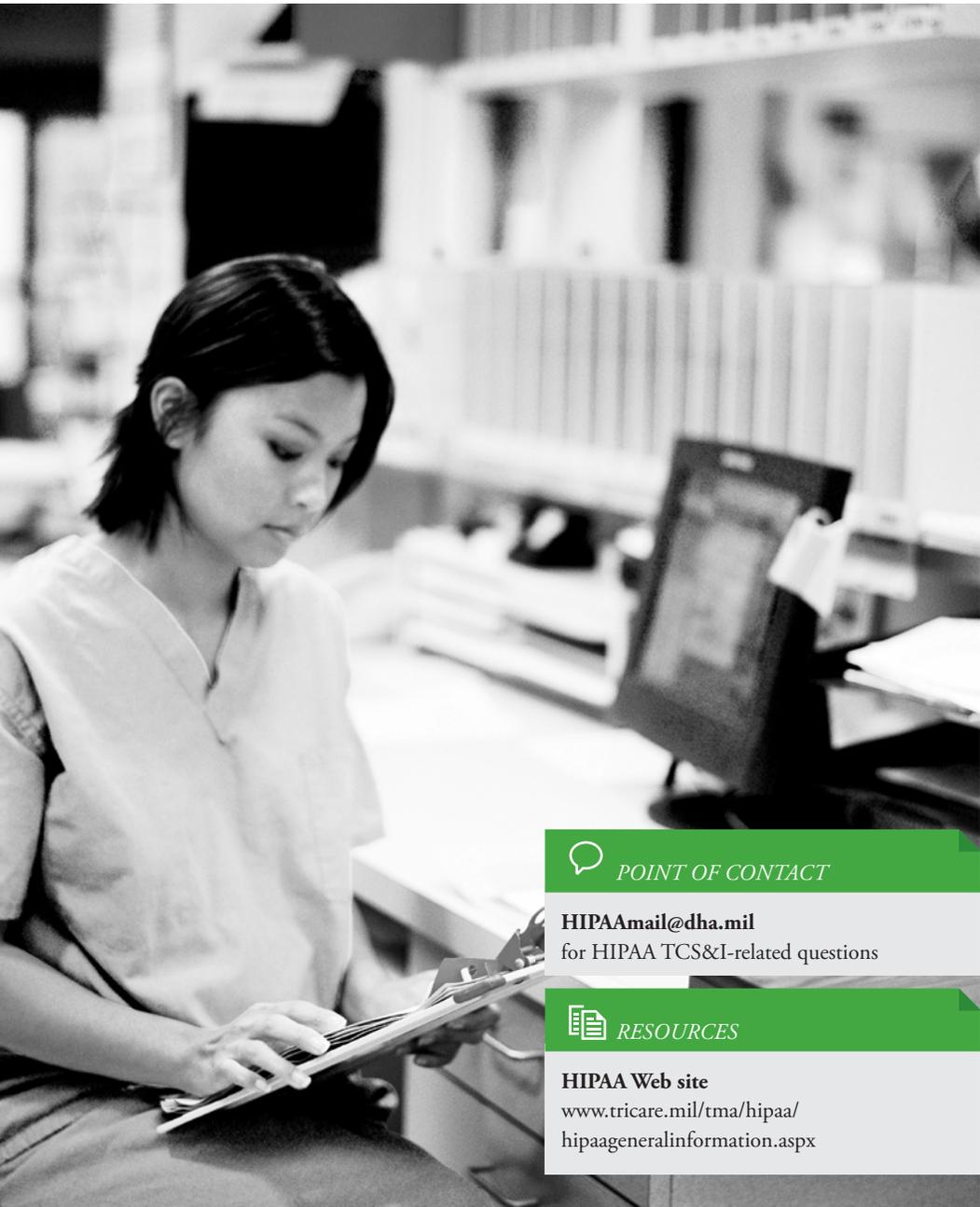
HIPAA also mandates the use of certain code sets within the HIPAA transactions. For example, ICD-10 (the International Classification of Diseases, 10th Edition Revision, and Clinical

Modification/Procedure Coding System) is a code set required by HIPAA. HIPAA TCS&I affects both TRICARE as a HIPAA covered health plan and as a provider.



### *WHICH COVERED ENTITIES NEED TO COMPLY?*

- Providers (e.g., military treatment facilities, civilian clinics, hospitals, individual 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 Enrollment Eligibility Reporting System/Defense Manpower Data Center, Managed Care Support Contractors)



### *POINT OF CONTACT*

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



### *RESOURCES*

**HIPAA Web site**  
[www.tricare.mil/tma/hipaa/hipaageneralinformation.aspx](http://www.tricare.mil/tma/hipaa/hipaageneralinformation.aspx)

# Data Sharing

## Requesting Access to Data Managed by DHA

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

### **DATA SHARING AGREEMENT (DSA) PROGRAM**

The Privacy Office uses the DSA process to:

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

### **DATA SHARING AGREEMENT APPLICATION (DSAA)**

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

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

**\* A DSAA MUST BE INITIATED BY THE FOLLOWING:**

**Applicant** – the individual who will provide primary oversight and responsibility for the handling of the requested data.

- For contract-driven requests, must be employee of 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.

## RESEARCH DATA SHARING STREAMLINING INITIATIVES

Streamlining measures are currently underway to prepare some enhanced multi-service markets (eMSM) for their MHS IRBs to take on the responsibility of conducting the required HIPAA Privacy Rule reviews and generating appropriate HIPAA-compliant documentation.

**\* THE RESEARCH DATA SHARING STREAMLINING MEASURES ARE:**

1. Create uniform MHS-wide HIPAA Privacy Rule Review templates
2. Develop agreements with select eMSMs and set conditions under which DHA Privacy Board review may no longer be required
3. Alleviate the current requirement for government personnel seeking data for research purposes to submit a DSAA (except in very limited cases)
4. Maintain the requirement of DSAA's for research-related contractors, but alleviate the need for DHA Privacy Board review in certain instances
5. Develop and accept overarching DSAA's from research foundations/organizations exclusively conducting research within eMSMs, thus eliminating the need for individual researchers to submit DSAA's



### *ARE YOU READY TO SUBMIT YOUR REQUEST?*

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

**Requests for data managed by DHA are reviewed for compliance with various data sharing requirements and must be submitted through a DSAA.**

### **DHA PRIVACY BOARD**

The DHA Privacy Board reviews research-related data requests for PHI for compliance with the HIPAA Privacy Rule.

There are four types of Privacy Board reviews:

1. Required Representations for Research on Decedent's Information – use or disclosure of PHI solely for research on decedents
2. Required Representations for Review Preparatory to Research
  - a. Use or disclosure of PHI solely for preparing a research protocol or similar purpose
  - b. Researchers agree not to remove PHI from DHA during review
3. Studies that must obtain HIPAA Authorizations
4. Studies that require a Waiver of Authorization or an Altered Authorization



## POINTS OF CONTACT

### **DSA.Mail@dha.mil**

for DSA-related questions

### **DHAPrivBrd@dha.mil**

for DHA Privacy Board-related questions

### **PrivacyMail@dha.mil**

for HIPAA Privacy-related questions



## RESOURCES

### **Enclosed CD**

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

### **DSA Web Page**

[www.tricare.mil/tma/privacy/duas.aspx](http://www.tricare.mil/tma/privacy/duas.aspx)

### **DHA Privacy Board Web Page**

[www.tricare.mil/tma/privacy/privacyboard.aspx](http://www.tricare.mil/tma/privacy/privacyboard.aspx)

### **DoD Health Information Privacy Regulation**

DoD 6025.18-R, January 2003

(currently under revision)

### **DoD Health Information Security Regulation**

DoD 8580.02-R, July 2007

(currently under revision)

# Human Research Protection Program

## Research Compliance

DoD supports and encourages research, including human subject research. All research protocols that include human subjects must be compliant with federal laws, federal regulations, and DoD policies intended to protect the subjects of the studies. The Human Research Protection Program (HRPP) provides guidance and enhances collaboration on research compliance issues.

### HRPP COMPLIANCE REVIEWS

The HRPP reviews compliance with:

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

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

- Initial review of approved protocols
- Requests to modify previously approved protocols
- Requests to continue a study beyond the expiration date of a previous approval

The HRPP office reviews protocols to determine if they meet the criteria for research on human subjects research and if so, conducts reviews to determine whether the research is exempt from IRB review. If exempt, the HRPP Office reinforces the understanding that the investigators must adhere to the ethical standards set forth in the Common Rule in order to provide research subjects with the greatest protection from harm.



### *HRPP COMPLIANCE REVIEWS*

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



### *HRPP TRANSITION*

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



### *POINT OF CONTACT*

**TMA\_HRPP@dha.mil**  
for HRPP-related questions



### *RESOURCES*

#### **Enclosed CD**

Please see the enclosed CD for a detailed presentation on Human Subject Research

#### **HRPP Web Site**

[www.tricare.mil/tma/privacy/hrpp/default.aspx](http://www.tricare.mil/tma/privacy/hrpp/default.aspx)

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

DoDI 3216.02, March 2002 (currently under revision)

# Breaches and Complaints

## Prevention and Mitigation

Equip yourself with a clear understanding of what breaches and complaints are, why they occur, and how to prevent them—it is the key to compliance with the Privacy Act of 1974 and HIPAA when faced with a potential violation. Mishandled or misused personally identifiable information (PII) or protected health information (PHI) can result in a breach or HIPAA Privacy violation, but the tips in this chapter can be a quick reference for methods to prevent breaches before they occur and how to mitigate breaches once they have been discovered. A critical element of breach and complaint management is the understanding of key definitions.

### WHAT IS A BREACH?

**Under the Privacy Act** and as defined by DoD, a breach is the “actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose.”

**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 (CE) or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

### WHAT IS A COMPLAINT?

A written statement submitted to a CE’s HIPAA Privacy Office, or to the HHS Office for Civil Rights (OCR), alleging that a CE has violated an individual’s health information privacy rights or committed a violation of the HIPAA Privacy, Security, or Breach Rule provisions.

#### **Substantiated complaint**

Investigation yields a violation of the HIPAA Privacy and/or Security Rule has occurred.

#### **Unsubstantiated complaint**

No evidence found to yield a violation of the HIPAA Privacy and/or Security Rule.

## HIPAA COMPLAINTS INVESTIGATION REPORT TEMPLATE

The information below is designed to assist with comprehensive and effective HIPAA Privacy complaint investigations. The investigation should include any other documentation or information requested by the DHA Privacy Office or HHS OCR (refer to the “checklist” enclosed with the original complaint) along with the following:

### 1. SUMMARY OF ALLEGATION(S)

- a. Statement of the allegation(s) being investigated
- b. Involved individuals, departments, offices, etc.

### 2. BACKGROUND/OVERVIEW OF INVESTIGATION

- a. Summary of investigation actions taken
- b. Interview records
- c. Sworn statements

### 3. ANALYSIS OF FACTS

- a. Clearly state how the investigative actions and findings relate to the allegation(s) of the complaint

### 4. CONCLUSION

- a. Statement of whether the allegations are substantiated or unsubstantiated
- b. Detail how the investigation findings support the conclusion/determination of the complaint
- c. If a determination cannot be made (i.e., due to insufficient evidence), provide an explanation as to why

### 5. MITIGATION ACTIONS

- a. Corrective and/or sanction actions including a current status (e.g., actions completed on MM/DD/YYYY or pending, etc.)

- b. Department training
- c. Counseling
- d. Policy and procedure revisions or development

### 6. DOCUMENTATION

- a. All relevant policies and procedures (e.g., uses and disclosures of PHI, safeguarding PHI, sanctions)
- b. Training records and/or certificates
- c. Apology and/or breach notification letter to the Complainant
- d. Documentation of imposed sanction actions, if applicable
- e. Documentation of training or changes made within the CE as a result of the investigation

### POLICIES AND PROCEDURES

Appropriate policies and procedures are critical in order to have an effective prevention and response management plan. An effective plan should include:

- Access, use, and disclosure of PII/PHI
- Safeguarding PII/PHI
- Breach reporting and complaint filing processes
- Comprehensive documentation (communications, requests, findings)
- HIPAA Privacy and Security training requirements

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



## BREACH PREVENTION TIPS

- Secure hard copy documents containing PII/PHI (e.g., lock your filing cabinet, desk, or office)
- Do not store PII/PHI on your laptop or any removable storage device unless authorized
- Log off when leaving your work station
- Familiarize yourself with the DHA fax policy to prevent an unauthorized disclosure (e.g., confirm recipient's fax number, use a coversheet, and confirm receipt)
- Encrypt e-mails containing PII/PHI when transmitting outside the network
- Be sure to redact all PII/PHI before distributing documents/files
- Close the door and/or lower your voice when discussing PII/PHI
- Double check an envelope prior to sealing it
- Disclose PII/PHI to only authorized individuals with an official need to know
- Never post PII/PHI on websites, especially social media
- Retrieve your documents from the printer promptly
- Validate all contact information prior to sending postal mail
- Do not leave your laptop unattended in your vehicle

*The above tips can also be used to avoid circumstances that lead to complaints.*



## BREACH REPORTING

Upon discovery of an actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information—where one or more individuals will be adversely affected—the breach must be reported according to the local incident response protocol.

FOR DHA	FOR SERVICE COMPONENTS
<b>LEADERSHIP:</b> Immediately	<b>LEADERSHIP:</b> Immediately
<b>US COMPUTER EMERGENCY READINESS TEAM:</b> Within 1 hour of discovery	<b>US COMPUTER EMERGENCY READINESS TEAM:</b> Within 1 hour of discovery
<b>DHA PRIVACY &amp; CIVIL LIBERTIES OFFICE:</b> Within 1 hour of discovery	<b>DOD COMPONENT SENIOR PRIVACY OFFICIALS:</b> Within 24 hours of discovery
<b>DEFENSE PRIVACY &amp; CIVIL LIBERTIES OFFICE:</b> Within 48 hours*	<b>DHA PRIVACY &amp; CIVIL LIBERTIES OFFICE:</b> Within 24 hours of discovery
<b>DEPARTMENT OF HEALTH AND HUMAN SERVICES*:</b> 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 impacted	<b>DEFENSE PRIVACY &amp; CIVIL LIBERTIES OFFICE:</b> Within 48 hours**

*\*DHA is responsible for reporting to the Defense Privacy and Civil Liberties Office and the Secretary of Health and Human Services.*

*\*\*The Service Components are responsible for reporting up their chain of command and to Defense Privacy and Civil Liberties Office.*

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 have been ascertained.

## THE SEVEN STEPS TO AN EFFECTIVE BREACH RESPONSE PLAN

### 1. BREACH IDENTIFICATION

Recognize that an event has occurred and initiate next step

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

### 2. BREACH REPORTING

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

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

### 3. CONTAINMENT

Limit the impact of the breach

- For electronic breaches, determine a course of action concerning the operational status of the compromised system, and identify the critical information and/or computing services affected by the breach
- 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 action may include:

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

### 5. ERADICATION

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

- Delete any computer viruses
- Update 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

## COMPLIANCE ENFORCEMENT

Enforcement of compliance should be reviewed and verified regularly.

- Include consequences and/or penalties for staff member non-compliance in employee manuals
- Retrain and provide remedial training on the appropriate privacy policies
- Consider stiffer penalties such as suspension, revocation of access, and/or termination
- Promote awareness consistently to prevent violations and breaches
- If the workforce sees little to no consequence for breaching PII/PHI, it may be less inclined to comply



## WORKFORCE TRAINING

Enforcement of staff training is essential to ensure compliance with the appropriate privacy and security policies. To do so:

- Confirm staff members are current with their annual Privacy Act and HIPAA 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 workforce is trained appropriately



## POINTS OF CONTACT

### **PrivacyOfficerMail@dha.mil**

to report breaches and for breach-related questions

### **PrivacyMail@dha.mil**

for HIPAA Privacy-related questions

### **HIPAASecurity@dha.mil**

for HIPAA Security-related questions



## RESOURCES

### **Enclosed CD**

Please see enclosed CD for detailed presentation on Breaches and Complaints

### **Breach Response Web Page**

[www.tricare.mil/tma/privacy/breach.aspx](http://www.tricare.mil/tma/privacy/breach.aspx)

### **HIPAA Privacy Web Page**

[www.tricare.mil/tma/privacy/hipaa-privacyrule.aspx](http://www.tricare.mil/tma/privacy/hipaa-privacyrule.aspx)

### **How to File a HIPAA Privacy Complaint**

[www.tricare.mil/tma/privacy/hipaa-PrivacyComplaint.aspx](http://www.tricare.mil/tma/privacy/hipaa-PrivacyComplaint.aspx)

# HIPAA Audits

## Audits Under HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires the Department of Health and Human Services (HHS) to conduct periodic audits to ensure covered entities (CE) and business associates (BA) comply with criteria associated with the HIPAA Privacy and Security Rules and Breach Notification standards. The HHS audit pilot program has ended and HHS is gearing up its HIPAA audit program for 2014 and beyond. CEs and BAs can prevent the loss of contracts, civil and criminal investigations, civil money penalties, and other adverse results that may result from an HHS audit by conducting robust reviews and assessments, mapping the movement of protected health information within their organizations, and complying with HHS guidance.

### TOP PRIVACY AND SECURITY PROBLEMS FROM HHS HIPAA AUDIT PILOT PROGRAM

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

## GETTING READY FOR AN AUDIT

Ensure you have the documentation required by the HIPAA Privacy and Security Rules, as implemented within DoD by DoD 6025.18-R and DoD 8580.02-R:

- Mapping of information security controls to the HIPAA Security Rule and DoD 8580.02-R standards and specifications
- A risk assessment conducted within the past 12 months and resulting risk management plan
- Continuity of operations plan
- Mapping your existing internal organizational procedures demonstrating full compliance with HIPAA Privacy Rule provisions

It is important to review the HIPAA Omnibus Final Rule issued by HHS in January 2013, which became effective in late September 2013 and the changes it made to the HIPAA Privacy, Security, and Breach Notification Rules. Use that review, as well as DHA Privacy Office breach notification guidance, to determine the changes, if any, needed to your organization's internal compliance procedures and processes. Then, make the necessary changes and document the changes made.

If you are at a military treatment facility, ensure you have documented how your organization handles access to or amendment of individual's health information, alternative communications, restrictions on disclosures, and accounting of disclosures.

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



## GOALS OF HITECH AUDIT PROGRAM

- Ensure CEs and BAs are complying with HIPAA Privacy and Security Rules and Breach Notification standards
- Spur CEs and BAs to assess and calibrate their privacy and security protections
- Permit the HHS Office for Civil Rights to develop best practices and guidance targeted to meeting observed compliance challenges
- Provide for overall improvement in CE and BA compliance with HIPAA standards



## POINT OF CONTACT

**PrivacyMail@dha.mil**  
for HIPAA Audit-related questions



## RESOURCES

### **DoD Health Information Privacy Regulation**

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

### **DoD Health Information Security Regulation**

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

# Military Command Exception

## Disclosing PHI of Armed Forces Personnel

In accordance with the HIPAA Privacy Rule and applicable DoD issuances, a DoD covered entity (CE) may use or disclose the protected health information (PHI) of Armed Forces members for activities deemed “necessary by appropriate military command authorities to assure the proper execution of the military mission.” This military command exception to HIPAA confidentiality protections denies when DoD providers may (1) disclose PHI of Service members to military commanders or (2) use PHI for military commanders’ purposes such as evaluating fitness for duty. If the specific requirements of this military command exception are satisfied, patient authorization is not required for such uses or disclosures. What follows is a summary of how the military command exception applies to DoD CEs. The military command exception as stated in 45 CFR 164.512(k)(1)(i) also applies to CEs outside of DoD, such as non-government hospitals and other health care providers. Those entities, however, are not subject to the DoD issuances referenced in this section.

### MILITARY COMMAND AUTHORITIES

Appropriate military command authorities include commanders who exercise authority over a member of the Armed Forces, or other 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).



### *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

## FURTHER DISCLOSURES

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

## ACCOUNTING OF DISCLOSURES

Disclosures to military commanders must be tracked for disclosure accounting purposes. See DoD Instruction (DoDI) 6025.18 for guidance.

Tracking is best accomplished by recording military command exception disclosures in the Protected Health Information Management Tool (PHIMT) at the time those disclosures are made.



[www.tricare.mil/tma/privacy/ProtectedHealthInformationManagementTool.aspx](http://www.tricare.mil/tma/privacy/ProtectedHealthInformationManagementTool.aspx)

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

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

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

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

## MEDICAL APPOINTMENT NOTIFICATION

Command authorities and/or their designees may require notification of medical appointments for Armed Forces personnel for purposes related to the execution of the military mission, such as fitness for duty determinations or assignment coverage. Medical appointment notifications include treatment reminders (physicals, immunizations, laboratory, etc.) and notifications of missed and cancelled appointments.

## 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.

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

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

## RECOMMENDED MTF POLICIES AND PROCEDURES

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

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

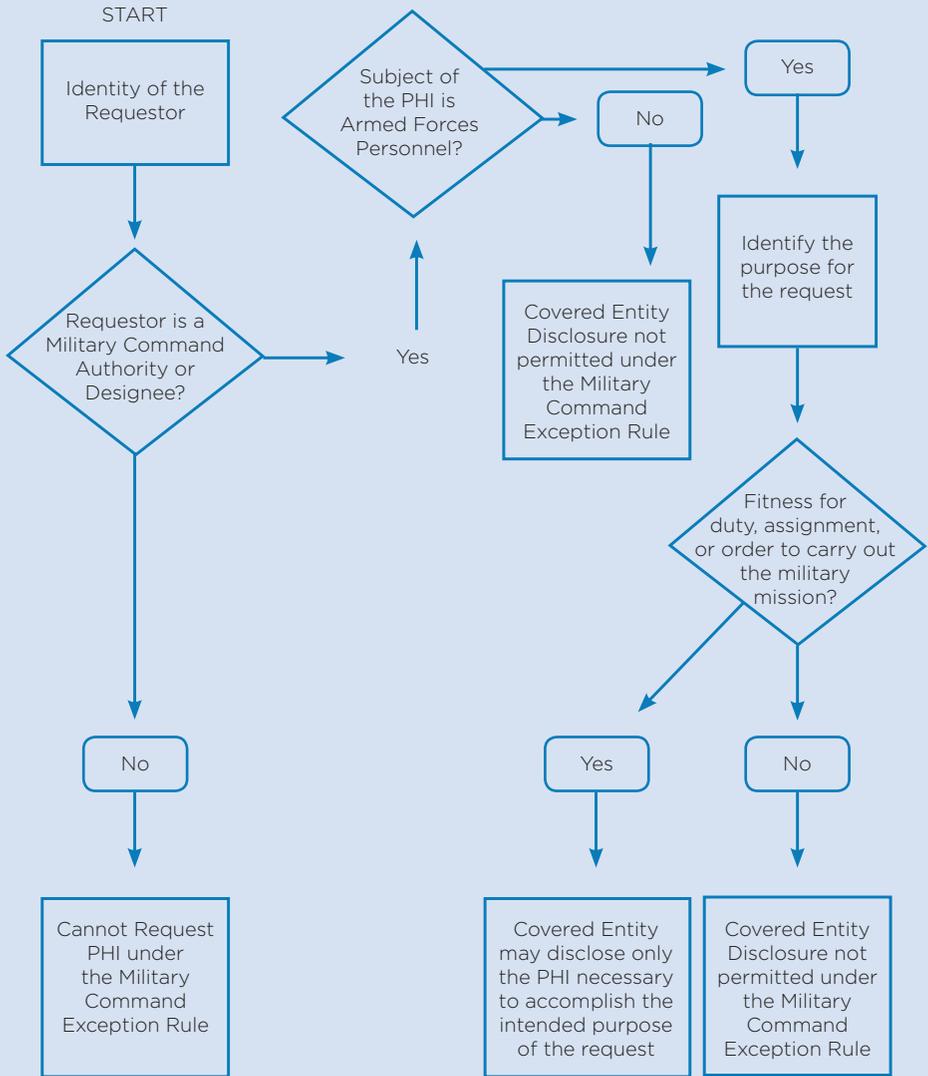


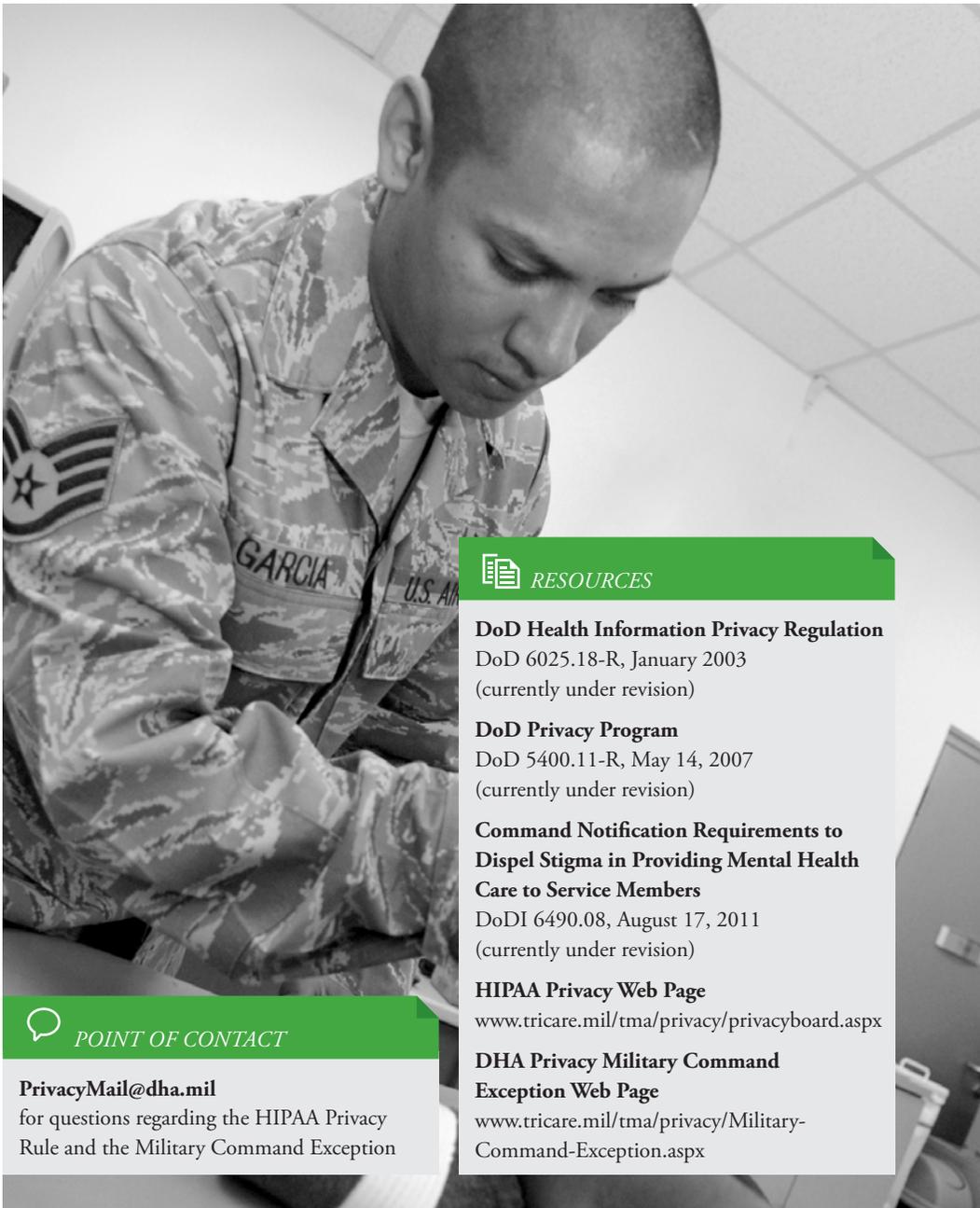
### *DISCLOSURE OF PHI RELATING TO MENTAL HEALTH CARE OR SUBSTANCE ABUSE TREATMENT*

Command notification by CEs is not permitted for Service member self and medical referrals for mental health care or substance misuse 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, recommended duty restrictions, and the prognosis.

# MILITARY COMMAND EXCEPTION DISCLOSURES





 **RESOURCES**

**DoD Health Information Privacy Regulation**

DoD 6025.18-R, January 2003

(currently under revision)

**DoD Privacy Program**

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**

[www.tricare.mil/tma/privacy/privacyboard.aspx](http://www.tricare.mil/tma/privacy/privacyboard.aspx)

**DHA Privacy Military Command Exception Web Page**

[www.tricare.mil/tma/privacy/Military-Command-Exception.aspx](http://www.tricare.mil/tma/privacy/Military-Command-Exception.aspx)



**POINT OF CONTACT**

**PrivacyMail@dha.mil**

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

# Health Information Exchange

## Sharing Health Data Electronically

Health Information Exchange (HIE) involves the capabilities needed to electronically share data among the key stakeholders in the health care system: patients, providers, and health plans. Because of DoD's ongoing need to exchange information with the Department of Veterans Affairs (VA) for over 9.6 million beneficiaries, DoD has been a leader in HIE for many years. To improve the quality of health care provided to beneficiaries, DoD is striving to increase the comprehensiveness of the data it exchanges along with expanding information sharing with other agencies and the private sector.

The Health Information Technology for Economic and Clinical Health (HITECH) Act 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 major HIE catalysts. HIE adoption 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 (PHR) by the two Departments.

The growth of electronic data exchange raises many significant privacy issues. Therefore, DoD has embarked on several initiatives to establish data sharing guidelines. DoD has taken steps to set expectations about the use and further disclosure of data once it is shared with both covered and non-covered entities. DoD uses various types of Data Sharing Agreements, such

as a Data Use Agreement (DUA), Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU), to establish and manage relationships with organizations. DoD is also implementing electronic capabilities to control data uses and disclosures that require consents or authorizations from individuals.

---

**“...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 V.A. health center. Their electronic records will transition along with them and remain with them forever.”**

President Barack Obama  
APRIL 9, 2009

---

EXCHANGE TYPE	WHAT IT COVERS
DoD INTERNAL Health Information Exchange	Health information exchanged internally to the DoD. Must be specific to a single patient AND must be electronic health record information
DoD INTERNAL Health Information Exchange Secondary data use	Health information exchanged internally to the DoD. Must be specifically aggregate information OR non-medical information
EXTERNAL Health Information Exchange Point-to-point / specific partner	Health information exchanged with a specific partner via a point-to-point method
EXTERNAL Health Information Exchange and Data Use and Reciprocal Support Agreement Publish / subscribe	Health information exchanged with private and governmental organizations that have signed the Data Use and Reciprocal Support Agreement
EXTERNAL Health Information Exchange Personal Health Record	Health information exchanged with the patient via the TRICARE Online Blue Button

## KEY HIE CAPABILITIES

### VIRTUAL LIFETIME ELECTRONIC RECORD (VLER)

VLER is a data exchange mechanism based on a query and response protocol that allows 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. Participating organizations include DoD, other governmental agencies, and private partners that have come together in an organization called the eHealth Exchange. Any participant can request data from an organization in the eHealth Exchange and receive data from other participant(s). DoD pilots are operational with an incremental roll out plan that aligns with the enhanced Multi-Service Markets (eMSM)

deployment strategy. There are approximately 40 other participants in the eHealth Exchange including the VA, Social Security Administration, and Kaiser Permanente. Each eHealth Exchange participant must sign the Data Use and Reciprocal Support Agreement (DURSA) which requires compliance with HIPAA Privacy and Security Rule requirements.

### HEALTH CARE ARTIFACT AND IMAGE MANAGEMENT SOLUTION (HAIMS)

HAIMS provides DoD and VA health care clinicians global access and awareness of radiographic images and documents generated during the health care delivery. HAIMS supports HIE by digitizing the paper components of the Service and non-Service Treatment Records and making the records available to the clinicians in the MHS as well as enabling DoD to meet

its obligation to provide the Service Treatment Record (STR) to Veterans Benefits Administration (VBA) partners in a paperless manner. There are two sets of digitization activities: one is directed at the day-to-day placement of documents into the medical record as they arrive at records offices; the other is directed specifically to the digitization of paper STRs.

### JOINT LEGACY VIEWER (JLV)

The JLV is currently deployed in pilot status to facilitate data exchanges between DoD and VA (including both Veteran's Health Administration [VHA] and VBA) and allows each organization to view the other's EHRs. The JLV provides VA with real time, direct access to the DoD STR and additional Military Treatment Facility (MTF) records. VHA uses the information for treatment purposes and VBA uses the records for benefits determinations. The current strategy is to expand the types of documents that are available for viewing and to increase the number of locations and individuals with access to the capability. It is anticipated that the VBA Appeals Management Center and Regional Offices will use the JLV once available.

### TRICARE ONLINE (TOL) BLUE BUTTON

TOL Blue Button allows authorized TOL users to view, download, and print their available personal health data. Users can populate a PHR of their preference or share data with family members, care givers, or other providers. They can also or keep/store the data as part of their PHR. Patients can access:

- Allergy profile (DoD and VA data)
- Medication profile (DoD and VA data)
- Laboratory results (DoD data)
- Problem lists (DoD and VA data)
- Encounters (DoD data)

### INTEGRATED ELECTRONIC HEALTH RECORD (iEHR)

DoD will acquire EHR capabilities and modernize legacy systems as necessary to achieve its goal of data interoperability with the VA. The iEHR will use standards defined by the Office of the National Coordinator for Health Information Technology. These standards will primarily focus on clinical and technical data requirements, but may also impact software and hardware capabilities and privacy and security policies that affect system development.



#### TEN CRITICAL QUESTIONS TO THINK ABOUT WITH ANY HIE

- ✓ How can using HIE save time?
- ✓ Will the exchange improve the quality of care delivered to patients?
- ✓ How will the exchange impact overall health care costs?
- ✓ Who will have access to the information?
- ✓ What security measures are in place to protect data and prevent breaches?
- ✓ Will the data for family members be shared through the exchange?
- ✓ Will all the covered entities participate in HIE?
- ✓ Will the exchange be operational at every location at the same time?
- ✓ Will someone conduct audits to ensure that confidential information is being protected?
- ✓ Is a patient required to participate in the exchange?

## DURSA REQUIREMENTS

There are selected DURSA requirements that are applicable to the MHS and other DURSA participants

- Messages may only be for permitted purposes, defined to include:
  - Treatment (of the individual who is the subject of the message)
  - Payment activities of that individual's provider, and certain other health care operations of the provider where the message recipient is that provider and the message topic is within specified categories
  - Public health activities and reporting
  - Demonstrating compliance with requirements of federal EHR incentive program
  - A purpose stated in HIPAA-compliant authorization by the individual who is the subject of the message
- Participant must determine its own Access Policies for determining whether and how to engage in messaging and establishing safeguards
- Participant must implement and maintain at least one of the types of information exchange services provided in the DURSA (these types are "submission, query and respond, publish and subscribe, and routing")
- In requesting messages for treatment, Participant has a reciprocal duty to respond to message requests for treatment. When messages are for Permitted Purposes other than treatment, responses are permitted but not required. Participant may temporarily cease messaging with another participant due to acts or omissions (e.g. a breach) of that other Participant, pending resolution under DURSA dispute resolution procedures
- In making a request based on an individual's HIPAA-compliant authorization, Participant is responsible for submitting a copy of the authorization
- Within one hour of discovering that a privacy breach may have occurred, Participant shall alert other Participants whose message content may have been breached. Within 24 hours after determining that a breach has occurred, a Participant shall notify other Participants likely impacted by the breach and the DURSA Coordinating Committee.



### *VLER HEALTH VIDEO*

[www.youtube.com/watch?v=a5UjdFfs\\_Yo&feature=c4-overview-vl&list=PLxyTToD6yJ7GIkfp6mZhgw3TpizO3Gt5v](https://www.youtube.com/watch?v=a5UjdFfs_Yo&feature=c4-overview-vl&list=PLxyTToD6yJ7GIkfp6mZhgw3TpizO3Gt5v)



## POINT OF CONTACT

### **PrivacyMail@dha.mil**

for questions related to health information exchange 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**

[www.tricare.mil/tma/privacy/hipaa.aspx](http://www.tricare.mil/tma/privacy/hipaa.aspx)

### **DoD Health Information Privacy Regulation**

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

### **HIPAA Privacy Rule**

45 CFR Parts 160 and 164

### **HIPAA Security Web Page**

[www.tricare.mil/tma/privacy/hipaa-securityrule.aspx](http://www.tricare.mil/tma/privacy/hipaa-securityrule.aspx)

### **HIPAA Security Rule**

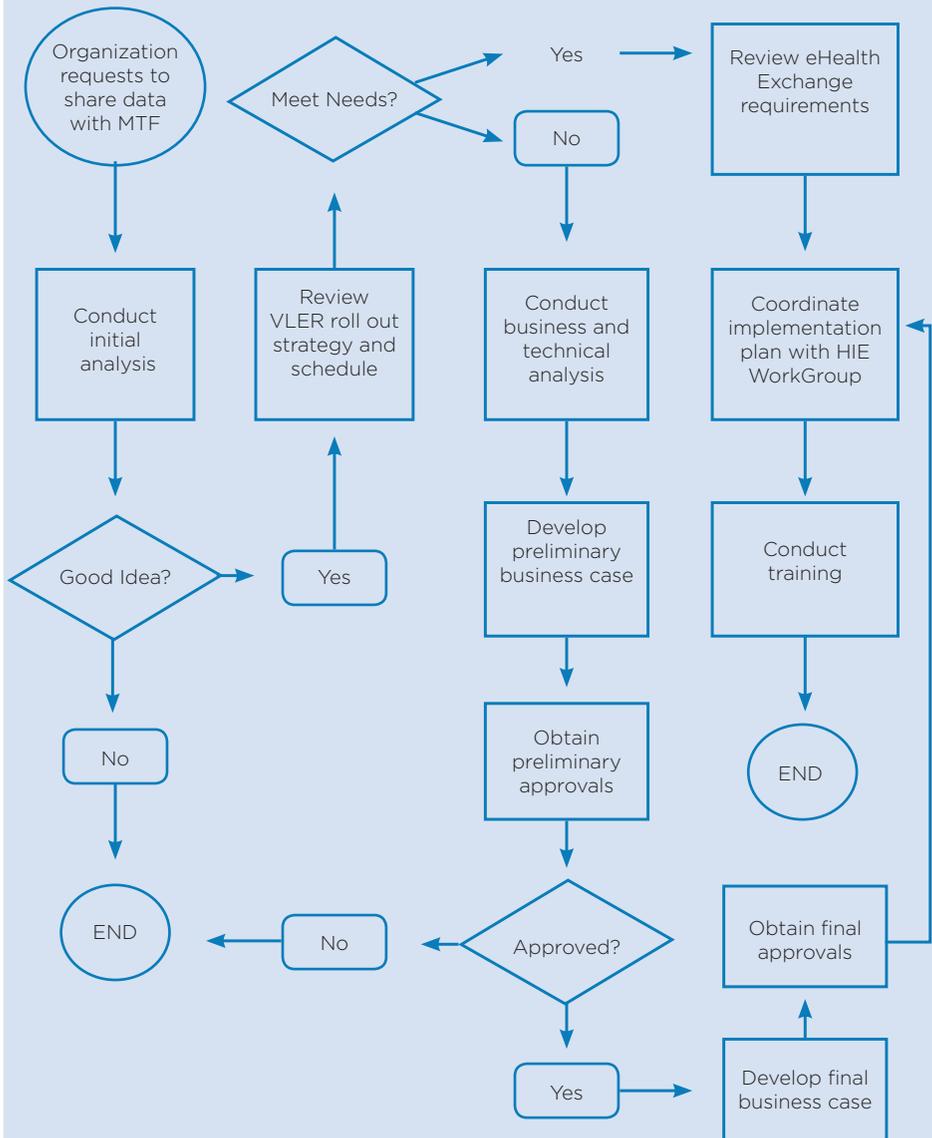
45 CFR Parts 160, 162 & 164

### **DoD Health Information**

### **Security Regulation**

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

## MTF/HIE DECISION PROCESS FLOW



# Federal Privacy Requirements Under the Privacy Act and E-Government Act

## Privacy Requirements Compliance

All federal executive branch agencies, whether a covered entity (CE) under HIPAA or not, must comply with general federal privacy requirements. These are chiefly mandated by the Privacy Act of 1974 and the E-Government Act of 2002, and associated regulations and guidance. DoD implements the Privacy Act with DoD 5400.11-R, DoD Privacy Program.

### THE PRIVACY ACT

The Privacy Act 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 was designed in part to embody the 1973 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

**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.

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

**Computer Matching Agreements** – When agencies have an agreement to compare two databases for benefits determinations or cost recoupment, specific procedures must be followed, including approval by an agency Data Integrity Board and publication in the Federal Register describing the data matching effort. Such agreements have time limits and must be re-reviewed before extensions can occur. The DHA has such an agreement with HHS Office for Civil Rights.

**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 account to the individual for disclosures made going back five years. The accounting must include to whom the information was disclosed and the date, nature, and purpose of the disclosure.

**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.

**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.

The Privacy Act provides for civil and criminal penalties under certain circumstances.

*NOTE – If your office deals regularly with information in a SORN, make sure all staff understand the specific routine uses in that system of records notice, and adhere to them fully.*



**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 (FIPPS) 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

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

In 2002, Congress passed the E-Government Act, which set forth many information technology (IT) requirements for executive agencies. The purpose of the Act is “to enhance the management and promotion of electronic government services

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

## MAIN E-GOVERNMENT ACT AND FISMA REQUIREMENTS

**Privacy Impact Assessments (PIAs) are required for systems.** Systems containing PII (especially regarding members of the public, but subsequent guidance has expanded this to PII regarding employees also) require a PIA. A PIA is a collaborative effort between the program office that operates and owns the system, the CIO's office including cyber security, and the Privacy Office, to ensure that the system complies with pertinent requirements and has adequately addressed any risk to privacy information. What is a "system" for PIA purposes? A system will generally be either a major application or a general support system, as defined by OMB Circular A-130, Appendix III. A major application is one requiring 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. Generally speaking, a system security plan is not required for minor applications because the protections associated with the larger systems generally already provide the appropriate security controls based on the general support system or major application in which they operate.

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

- What information is collected
- Why collected

- Intended use of 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

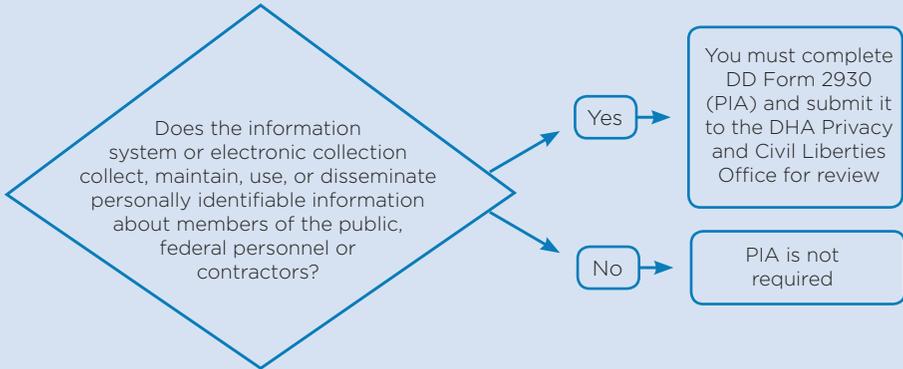
### **Privacy policies of agencies must be in "machine-readable" formats.**

**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 Privacy Act and HIPAA 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.

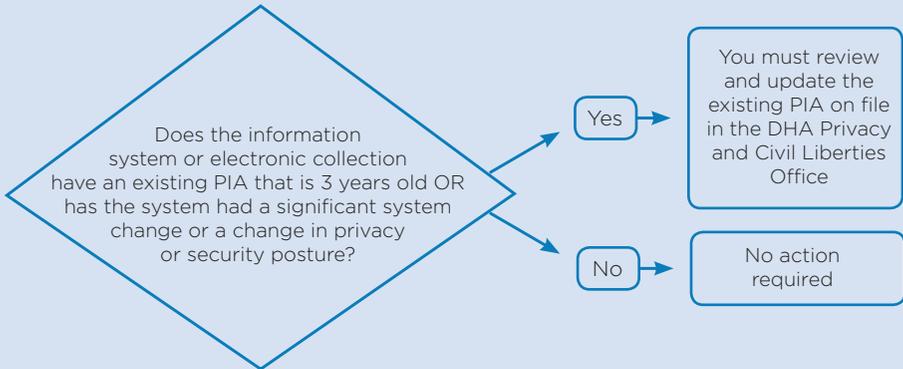
### **Annual reporting on compliance with Privacy Act and E-Government Act requirements.**

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 completion of system of records notices and privacy impact assessments of the agency, among other data elements.

## DO I NEED A PRIVACY IMPACT ASSESSMENT (PIA)?



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

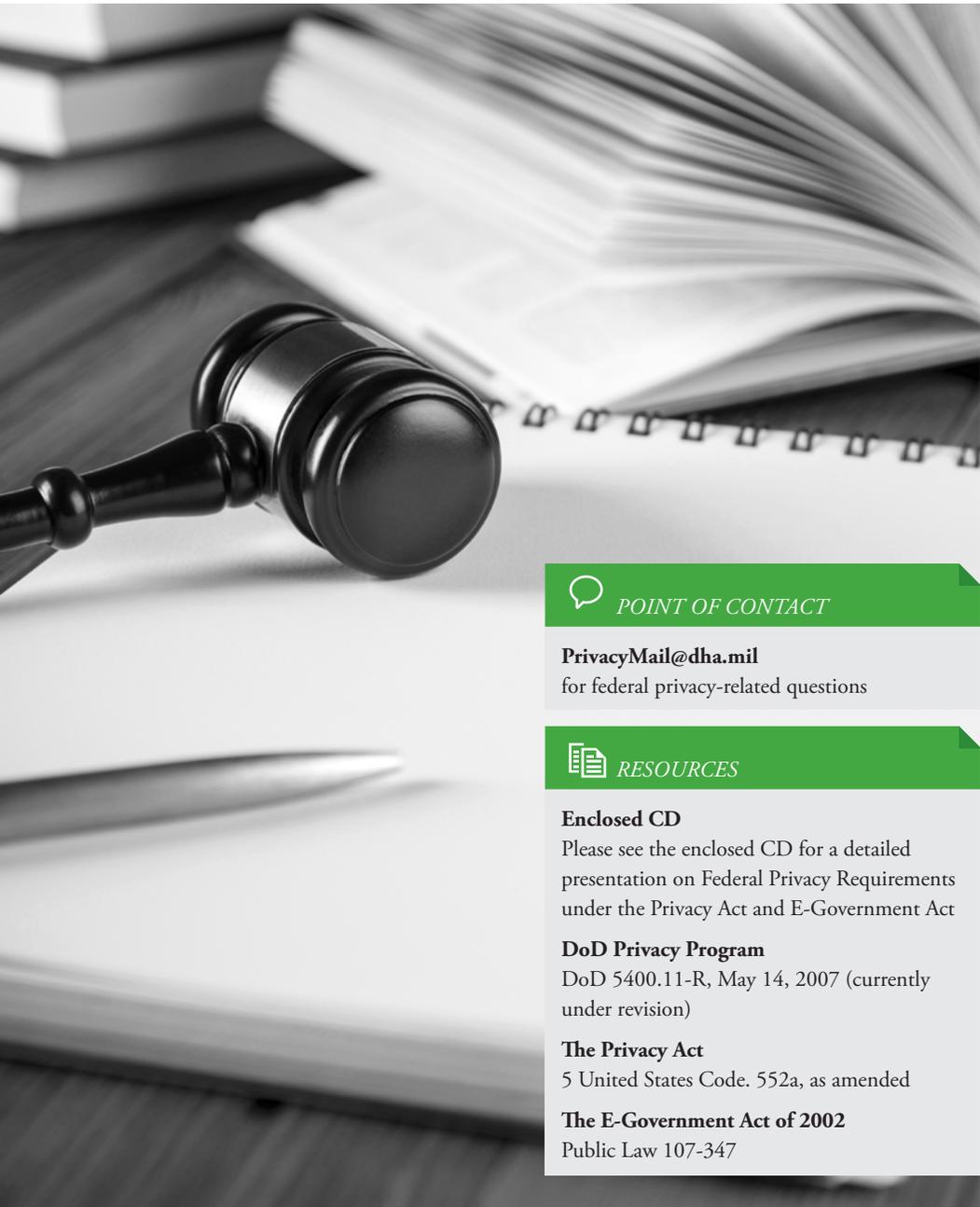


## DO I NEED A SYSTEM OF RECORDS NOTICE (SORN)?

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

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

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 ([www.tricare.mil/tma/privacy/privacyact.aspx](http://www.tricare.mil/tma/privacy/privacyact.aspx)).



### *POINT OF CONTACT*

**PrivacyMail@dha.mil**

for federal privacy-related questions



### *RESOURCES*

**Enclosed CD**

Please see the enclosed CD for a detailed presentation on Federal Privacy Requirements under the Privacy Act and E-Government Act

**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 Model Civil Liberties Program

## Safeguarding Civil Liberties

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.

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 appoint a senior official to advise on civil liberties and meet certain statutory requirements. Therefore, the Director of Administration and Management, was appointed to serve as the DoD Civil Liberties Officer (CLO), and instructed DoD components to review the placement of civil liberties within their organizations and designate a civil liberties office and CLO. On January 26, 2011, the Privacy Office’s name was changed to the TRICARE Management Activity Privacy and Civil Liberties Office. As of October 1, 2013, with the establishment of the DHA, the office is now the DHA Privacy and Civil Liberties Office (Privacy Office).

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 DHA employees’ and contractors’ work may have on an individual’s civil liberties, please reach out to the Privacy Office for guidance.

### KEY TERMS

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

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

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

## BILL OF RIGHTS

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

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

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



### *CIVIL LIBERTIES BEST PRACTICES*

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

 **RESOURCES****Enclosed CD**

Please see the enclosed CD for a detailed presentation on the DHA's Model 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)

**DoD Health Information Security Regulation**

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

**Civil Liberties Program Case Management System**

Director of Administration and Management  
01, January 19, 2011

**DHA Civil Liberties Program**

DHA Administrative Instruction, Number 64,  
April 24, 2013

**POINT OF CONTACT**

**Civil\_Liberties@dha.mil**

for DHA civil liberties-related questions

# The Freedom of Information Act

## Public Access to Information

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 that are pending at an agency at the end of the fiscal year that 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 in 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 Grant** – An agency decision to disclose all records in full response to a FOIA request.

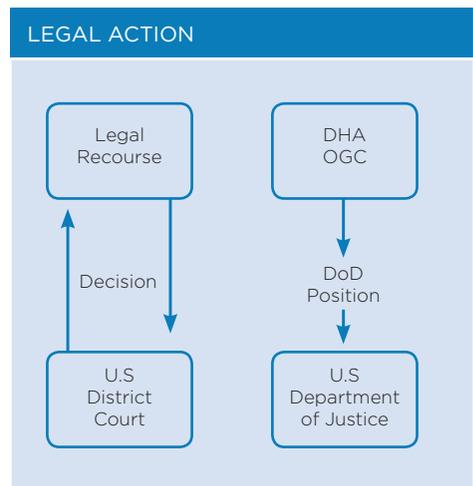
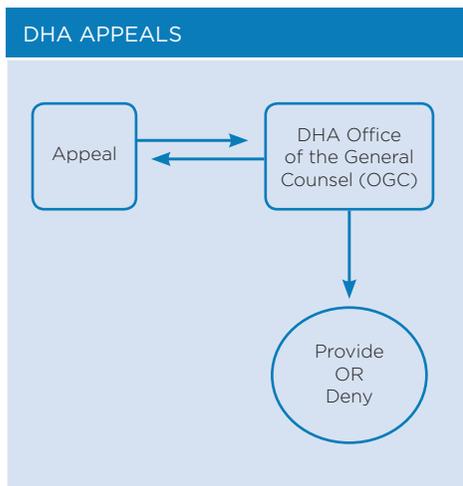
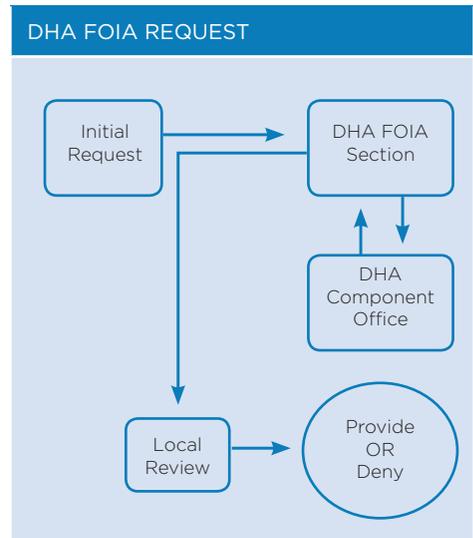
**Full Denial** – An agency decision not to release any records in response to a FOIA request because the records are exempt in their entireties under one or more of the FOIA exemptions, or because of a procedural reason, such as when no records could be located.

**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.

**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.





## 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

## PRIVACY ACT OF 1974

The Privacy Act of 1974 establishes safeguards for the protection of records that the Federal Government collects and maintains on United States citizens and aliens lawfully admitted for permanent residence. Specifically, it mandates that the United States Government:

- Disclose why information is being collected and how it will be used
- Maintain only what is needed to accomplish agency business
- Publish any new, revised, or deleted system notices in the Federal Register
- Ensure that information is accurate, relevant, and complete
- Provide individuals with the opportunity to correct inaccuracies in their record

### **The Privacy Act allows individuals to:**

- Seek access to records retrieved by their name and personal identifier
- 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

 **RESOURCES****Enclosed CD**

Please see the enclosed CD for a detailed presentation on FOIA

**Exemptions and/or the FOIA Process**

[www.tricare.mil/tma/privacy/foia.aspx](http://www.tricare.mil/tma/privacy/foia.aspx)

**FOIA Electronic Reading Room**

[www.tricare.mil/tma/privacy/FOIAeletic.aspx](http://www.tricare.mil/tma/privacy/FOIAeletic.aspx)

**Appeals or Complaints**

[www.tricare.mil/tma/privacy/Appeals.aspx](http://www.tricare.mil/tma/privacy/Appeals.aspx)

**White House Presidential Memorandum FOIA**

[www.whitehouse.gov/the\\_press\\_office/Freedom\\_of\\_Information\\_Act/](http://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](http://www.usdoj.gov/oip/amendment-s2488.pdf)

**DoD Privacy Program**

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

**POINT OF CONTACT**

**[FOIARquests@tma.osd.mil](mailto:FOIARquests@tma.osd.mil)**

for FOIA-related questions or for requester status updates





