

HEALTH INFORMATION PRIVACY AND SECURITY

TRAINING MANUAL

JUNE 2018



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

DHA PRIVACY AND CIVIL LIBERTIES OFFICE

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

This Training Manual is a product of the DHA Privacy Office's training and awareness program, published annually, and authored by privacy and security subject matter experts throughout the Military Health System. It contains an overview of key programs, guidelines, initiatives, and tools that will help navigate the complex and demanding world of privacy and Health Insurance Portability and Accountability Act (HIPAA). It also includes recent privacy-related policy updates, process flow charts and diagrams, relevant resources, and contact information for each topic area.

As privacy and security continue to be focus areas across organizations, and especially in the Federal Government, the DHA Privacy Office continues to be a leader in privacy compliance for DHA. The DHA Privacy Office is fully invested in protecting privacy, ensuring HIPAA compliance, supporting compliance in data sharing and human research protection, fulfilling Freedom of Information Act requests and potential breaches, and promoting Civil Liberties.

We look forward to continuing to work with all DHA personnel and cultivating a culture of privacy protection through efforts such as our annual Health Information Privacy and Security Training. This Training Manual supports these outreach efforts, serving as a reference for all privacy-related matters. The Training Manual may also be accessed electronically on the DHA website at: <http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Act-and-HIPAA-Privacy-Training/Training-and-Awareness>.

Finally, I would like to thank my talented and dedicated team for all they do to support the DHA Privacy Office. Please do not hesitate to reach out to us, and I appreciate your ongoing efforts to protect the information of which we are entrusted.

Sincerely,

Rahwa A. Keleta

Acting Chief, DHA Privacy and Civil Liberties Office



MAILING ADDRESS

Defense Health Headquarters
7700 Arlington Boulevard
Suite 5101
Falls Church, VA 22042

OFFICE LOCATION

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



TABLE OF CONTENTS

Introduction.....	2
Federal Privacy Requirements Under the Privacy Act and E-Government Act.....	5
HIPAA Privacy.....	14
HIPAA Security.....	23
HIPAA Transactions, Code Sets, and Identifiers.....	31
Privacy and Risk Management.....	34
Data Sharing.....	38
Human Research Protection Program.....	43
Breach Response.....	48
Military Command Exception.....	55
MHS GENESIS and Other Emerging Technologies.....	62
DHA's Civil Liberties Program.....	66
Freedom of Information Act.....	71



INTRODUCTION

Defense Health Agency

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

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



DHA was established in October 2013. The idea of DHA stemmed from a long-held conviction that military health care could be better integrated and more efficient. With the Presidential signing of the 2017 National Defense Authorization Act, DHA is poised to take on an even greater role in military health and increase collaboration across the MHS and the Services. This will have an impact across every division and directorate of DHA, including the DHA Privacy and Civil Liberties Office (Privacy Office), especially given its role in safeguarding personally identifiable information (PII) and protected health information (PHI).

DHA supports the Quadruple (QUAD) Aim goals, which are as follows: increased readiness, better health, better care, and lower cost.

THE QUADRUPLE AIM

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



Vice Admiral (VADM) Raquel Bono, the Director of DHA, has set DHA priorities and goals to further the QUAD Aim key points and is focused on promoting DHA as an Integrated System of Readiness and Health that is 'unified and ready.'

Among VADM Bono's goals for the agency are to: empower and care for our people; optimize operations across the MHS; co-create optimal outcomes for health, well-being and readiness; and deliver solutions to combatant commands. The DHA Privacy Office fully supports these goals, and sees its mission of privacy protection as supporting these aims.

DHA PRIVACY AND CIVIL LIBERTIES OFFICE

The DHA Privacy Office, which falls under DHA J-1, the Administration and Management Directorate, oversees the protection of PII and PHI within the MHS. The MHS is one of the largest integrated healthcare delivery systems in the United States, serving over 9.4 million eligible beneficiaries around the world. The DHA Privacy Office supports MHS compliance with federal privacy and Health Insurance Portability and Accountability Act (HIPAA) laws, and DoD regulations and guidance. This includes managing and evaluating potential risks and threats to the privacy and security of MHS health data by performing critical reviews through:

- Evaluation of privacy and security safeguards, including conducting annual HIPAA of 1996 Security Risk Assessments
- Performance of internal DHA Privacy Office Compliance Assessments
- Establishment of organizational performance metrics to identify and measure potential compliance risks
- Consultation for leadership and the workforce on areas of DHA-level oversight

In addition, the DHA Privacy Office has specific responsibilities for various DHA-level areas.

Key elements include:

- Breach Prevention and Response
- HIPAA Privacy and Security
- Privacy Act of 1974
- Freedom of Information Act
- Data Sharing Compliance
- Human Research Protection
- Upholding Civil Liberties
- Emerging Technology trends and compliance

The DHA Privacy Office also engages MHS stakeholders, including employees and contractors, by developing and delivering education and awareness materials and ongoing workforce privacy and HIPAA security training.



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

Privacy Requirements Compliance

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

THE PRIVACY ACT

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

MAIN PRIVACY ACT REQUIREMENTS

Access and Amendment of Records –

Privacy Act Request: An individual may generally be provided access to, and a copy of, information about that person from a Privacy Act SOR upon written request. The individual may also seek amendment of information about him or herself upon proof of inaccuracies. The DHA Privacy Office administers Privacy Act requests for DHA-managed information.



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

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

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



Privacy Act Statement (PAS) – When asking individuals to supply PII that will become part of a SOR, DHA is required to provide a PAS on the form used to collect the information or on a separate form that can be retained by the individual. DHA must provide a PAS in such circumstances regardless of whether the information will be collected in paper or electronic form, on a website, on a mobile application, over the phone, or through some other medium. Web forms must display the PAS prominently. The PAS must include, in plain language, the authority for collecting the information (i.e., a statute or executive order); the principle purpose for which the information is intended to be used; whether providing PII is mandatory or optional; the intended disclosures or published routine uses to which the information is subject; the effects on the individual, if any, of not providing all or any part of the requested information and an appropriate citation (and if applicable, a link) to the relevant System of Records Notices (SORNs).

NOTE: A form is considered voluntary unless failure to complete it violates a law or regulation. An example of an involuntary form is a required tax form.

System of Records Notice (SORN) – A SORN is a notice published by an agency in the Federal Register upon the establishment and/or modification of a SOR describing the existence and character of the system. SORNs must also be published on the agency's website.

A SOR 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, symbol, or other identifying particular assigned to the individual.” The SORN identifies the SOR, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the intended disclosures

of PII or the routine uses to which the records are subject, safeguards used to protect the confidentiality of that system, and additional details about the system. The requirement for agencies to publish a SORN allows the Federal Government to accomplish one of the basic objectives of the Privacy Act – to foster agency accountability through public notice.

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

THE FAIR INFORMATION PRACTICE PRINCIPLES INCLUDE:

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

Transparency	Agencies provide notice of systems collecting PII, and information about those systems including purposes and uses
Individual Participation	Individuals may access their own information from a SOR, and may 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 the data 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

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

The Privacy Act ensures that agencies do not disclose any record by any means of communication to any person or to another agency, except at the request of the individual to whom the record pertains via written consent. Nevertheless, there are 12 exceptions to this requirement. Sharing PII without such consent may occur when sharing:

1. 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. Solely for statistical research or reporting record, and transferred in a form not individually identifiable
6. To the National Archives and Records Administration when historical interest warrants
7. To another United States 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

In addition to the 12 exceptions, Office of Management and Budget (OMB) M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017), ensures that agencies share information to respond to agency breaches, whether it is to respond to a breach of either the agency’s PII, or as appropriate, to assist another agency in its response to a breach.



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 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.” There are some key privacy-related requirements for agencies within the E-Government Act.

MAIN E-GOVERNMENT ACT AND FISMA REQUIREMENTS

According to the E-Government Act and FISMA of 2002, as well as DoD 5400.16, Privacy Impact Assessments (PIAs) are required for all Federal information systems that collect, maintain, and disseminate PII. Federal information systems containing PII (especially regarding members of the public, but subsequent guidance has expanded this to PII regarding employees as well) require a PIA. A PIA is a collaborative effort between the program office that operates and owns the information system, the CIO’s office including the Cyber Security Division, and the DHA Privacy Office, to ensure IT complies with all pertinent requirements and adequately addresses any risk to privacy information.

What is a “Federal information system” for PIA purposes?

The E-Government Act defines a federal information system as “an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.” The National Institute of Standards and Technology (NIST) Act describes an information system as a “discrete set of information resources (information and related resources, such as personnel, equipment, funds, and information technology) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.” Moreover, the revised OMB Circular A-130, *Managing Information as a Strategic Resource* (July 16, 2016), likens an information system to an information technology.

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

- What information is collected
- Why the information is collected
- Intended use by the agency
- With whom it will be shared
- What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared
- Rights of the individual under the Privacy Act
- Any related information

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

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

and HIPAA Security Officer training for those filling such roles throughout the MHS. Contact the DHA Privacy Office for further information.

Annual reporting on compliance must occur 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 on security systems compliance, and a section on privacy compliance including information on the completion of SORNs and PIAs of the agency, among other data elements.

DO I NEED A SORN?	
If a 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	Is the information about an individual collected, maintained, or used by DoD or a contractor on DoD’s behalf? ✗ Answer no if only collected to verify a person’s identity and then deleted
2	If the answer to question 1 is yes, does the information collected include PII? ✓ Answer yes even if the individual is an employee or Service member
3	If the answer to question 2 is yes, is the information retrieved by the individual’s unique identifier? ✗ Answer no if the system can retrieve by a unique identifier, but does not ✗ Answer no if the system only retrieves by non-unique identifiers such as a case number ✗ Answer no if the system only retrieves by a unique identifier when an individual asks for his or her own records
Note that the form of the information (paper, electronic, or combination) does not matter. For further guidance on SOR and SORN selection, please visit the DHA Privacy Office website (http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties).	

DO I NEED A PIA?

If the information system does not have an existing PIA, the program manager, system owner, or designee must complete a privacy threshold analysis (PTA)¹. The DHA Privacy Office will determine whether PII is collected and a PIA is required.

? Is PII collected?

Did the DHA Privacy Office determine whether a PIA is required?

NO



PIA is not required.

YES



The program manager, system owner, or designee must complete DD Form 2930 (PIA) and submit it to the DHA Privacy Office for review.

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

Does the information system or electronic collection have an existing PIA that is three years old or has the system had a significant system change or a change in privacy or security posture?

NO



No action required.

YES



The program manager, system owner, or designee must review and update the existing PIA on file with the DHA Privacy Office.

¹ The DHA Privacy Program Plan requires a PTA to be performed as the first step in determining whether PII exists on a system, whether a PIA is needed, whether a SORN is required, and if other privacy requirements are needed.

INTERCONNECTEDNESS

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

- When conducting a survey
- When posting information online
- When contracting for services
- When sharing information between agencies
- When acquisitioning IT

Please remember to consult with the DHA Privacy Office if you have any questions!

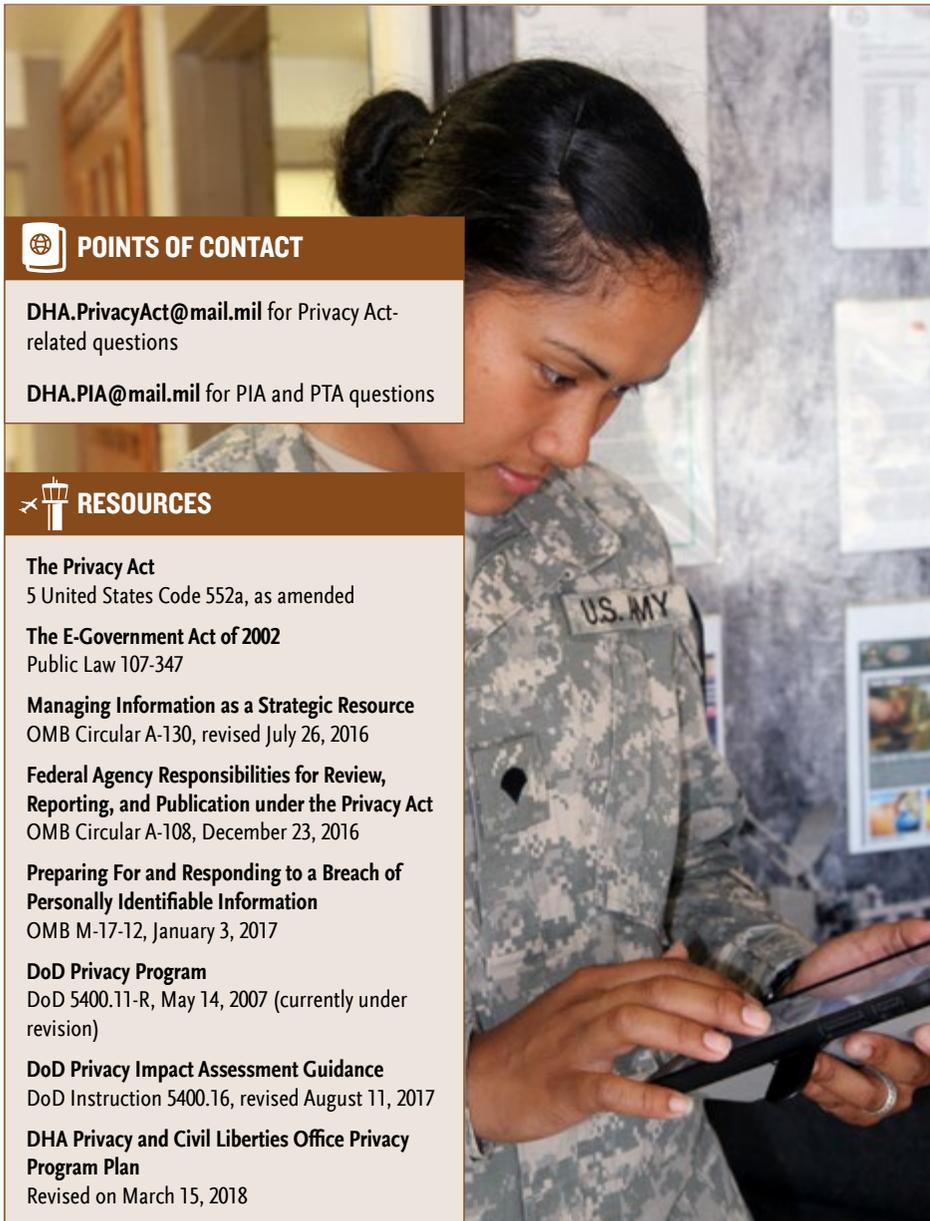


LOOKING AHEAD

Federal Privacy Updates
DoD is moving towards having one Privacy Act rule, which aligns with OMB Circular A-108's Privacy Act implementation and exemption rules for implementing requirements under the Privacy Act. The policy enforces a number of accompanying concepts such as the continuous monitoring of SORNs, Privacy Act exemptions, and the Federal Acquisition Regulation Council issuance of instructions regarding what agencies must do to comply with the requirements of the Privacy Act and privacy training (as demonstrated in Circular A-108).

Revision 5 (Rev. 5) of NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, is set to be published in 2018. In addition to establishing SORN and PIA as separate privacy controls, Rev. 5 clarifies the relationship between security and privacy, and fully integrates the privacy controls into the security catalog.

For more information, please visit the Federal Privacy Council (FPC) one-stop-shop website for all privacy professionals at <https://www.fpc.gov/>. The FPC was established in 2016 as a result of President Obama's February 9th Executive Order, *Establishment of the Federal Privacy Council*, to serve as an interagency support structure that provides a plethora of useful privacy laws, mandates, guides, and other information and resources to improve practices among federal agencies.



POINTS OF CONTACT

DHA.PrivacyAct@mail.mil for Privacy Act-related questions

DHA.PIA@mail.mil for PIA and PTA questions

RESOURCES

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

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

Managing Information as a Strategic Resource
OMB Circular A-130, revised July 26, 2016

Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
OMB Circular A-108, December 23, 2016

Preparing For and Responding to a Breach of Personally Identifiable Information
OMB M-17-12, January 3, 2017

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

DoD Privacy Impact Assessment Guidance
DoD Instruction 5400.16, revised August 11, 2017

DHA Privacy and Civil Liberties Office Privacy Program Plan
Revised on March 15, 2018

HIPAA PRIVACY

Complying with the HIPAA Privacy Rule within the MHS

Safeguarding the privacy and security of health information is a key focus of the HIPAA Privacy Rule, issued by the Department of Health and Human Services (HHS) in 2002, and updated in the HIPAA Omnibus Final Rule in 2013. The HIPAA Privacy Rule applies to covered entities (CEs), including health plans, healthcare clearinghouses, and healthcare providers who transmit any health information in electronic form in connection with a HIPAA transaction. The HIPAA Privacy Rule provides a federal floor of minimum standards that govern the uses and disclosures of protected health information (PHI) as well as patient rights with respect to PHI created, disclosed, or received by CEs or their business associates (BAs). The MHS must comply with the requirements of the HIPAA Privacy Rule, both as a provider of health care and as a health plan through the TRICARE Program.

DoD implements the HIPAA Privacy Rule through DoD 6025.18-R, the DoD Health Information Privacy Regulation, dated January 24, 2003. This issuance is currently under revision and will be reissued as a DoD Instruction (DoDI) and corresponding DoD Manual (DoDM). Upon publication of the updated guidance, the DHA Privacy Office will release a mapping between DoD 6025.18-R and the DoDM to help familiarize stakeholders with the updated content and organization. A summary of notable changes is included later in this chapter.

KEY TERMS

Business Associate (BA) – A person or entity who is not a member of the CE's workforce and who provides a service for or on behalf of the CE that involves the use or disclosure of PHI. DoD CE BAs may include other DoD CEs, DoD components, and other governmental and non-governmental entities under contract with DoD. See DoD 6025.18-R, paragraph C3.4.1.

Business Associate Agreement (BAA) – A legal agreement between a CE and its BA that establishes the permitted and required uses and disclosures of PHI by the BA, obtains certain promises from the BA, and authorizes the termination of the BA when a material term has been violated. Requirements for DoD CE BAAs are set forth in DoD 6025.18-R, paragraphs C3.4.2 and C3.4.3. Approved BAA language and formats for use by DoD CEs is available at <http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language>.

Covered Entity (CE) – A health plan, healthcare clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a HIPAA transaction. CEs within DoD are generally defined or identified in DoD 6025.18-R, paragraph C3.2.

Disclosure – The release, transfer, provision of access to, or other divulging in any 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 accomplish the intended purpose of the use, disclosure, or request. Exceptions to this standard are as follows:

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

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

Organized Health Care Arrangement (OHCA) – An organized system of health care in which participating CEs hold themselves out to the public as participating in a joint arrangement and in certain joint activities. The MHS and certain elements of the United States Coast Guard are designated an OHCA, under DoD 6025.18-R C3.3. This status allows members of the OHCA to exchange PHI with each other for treatment, payment, and healthcare operations (TPO) purposes, have a joint NoPP, and share a common BA.

Protected Health Information (PHI) – Health information created by or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that relates to the individual's past, present, or future physical or mental health, the provision of health care, or the payment for health services, and that identifies the individual or it is reasonable to believe the information can be used to identify the individual. PHI excludes information contained in employment records held by a CE in its role as an employer, education records covered by the Family Educational Rights and Privacy Act, and regarding a person who has been deceased for more than 50 years. Because DoD is a federal agency, PHI of a DoD CE is also personally identifiable information under the Privacy Act of 1974.

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

PATIENT RIGHTS UNDER THE HIPAA PRIVACY RULE

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

Under HIPAA, patient rights include:

RIGHT TO A NoPP

Individuals have a right to adequate notice of the uses and disclosures of their PHI that may be made by the CE and of the patients' rights and the CE's legal duties with respect to their PHI. See DoD 6025.18-R, Chapter 9.

RIGHT TO REQUEST RESTRICTIONS

Individuals have a right to request that a CE restrict the use or disclosure of their PHI for TPO purposes or to persons involved in the individuals' care or healthcare payment. A CE is not required to agree to a restriction request, except for a request to restrict disclosure of PHI to a health plan if the PHI is related to a service or product for which the individual has paid out-of-pocket in full. A CE may break an agreed-upon restriction if the PHI is needed for emergency treatment, or if the CE informs the individual in writing. Acceptance, denial, and/or termination of a restriction must be documented by the CE. DoD 6025.18-R, paragraph 10.1, provides information on the process and procedures to be followed by a DoD CE receiving such a request.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

Individuals have a right to request that their PHI be communicated in a certain way or at a certain location (e.g., only at home or only by postal mail). A covered healthcare provider must accommodate reasonable requests to communicate PHI by alternative means or at alternative locations. A covered health plan must accommodate reasonable requests only if the individual clearly states that the disclosure of all or part of the PHI could endanger the individual. DoD 6025.18-R, paragraph 10.2, provides guidance as well as requirements for DoD CEs in connection with documenting and responding to a request for confidential communications.



RIGHT TO INSPECT AND COPY

Individuals have a right of access to inspect and obtain a copy of their PHI held by a CE in a designated record set (including an electronic copy, if maintained electronically). See DoD 6025.18-R, Chapter 11. A DoD CE may deny such requests, with respect to the following PHI in a designated record set:

- Psychotherapy notes
- PHI compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
- Quality assurance information
- Information related to an inmate if it would jeopardize the individual, other inmates, or correctional institution or transportation staff
- PHI created or obtained in the course of research where the individual has previously agreed not to access the information while the research is in progress
- Information subject to the Privacy Act if the denial would satisfy Privacy Act requirements – for example, records classified in the interest of national defense or foreign policy, and certain investigatory material
- PHI obtained from someone other than a healthcare provider under a promise of confidentiality, and the release of the information would likely reveal the source

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

- A licensed healthcare professional determines that the access requested is reasonably likely to endanger the life or safety of the individual or another person
- The PHI references another person, other than a healthcare provider, and a licensed healthcare professional determines that access is reasonably likely to cause substantial harm to such person
- The request is made by the individual's personal representative and a licensed healthcare professional determines that the representative's receipt of the PHI is reasonably likely to cause harm to the individual or another person

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

If access to PHI is denied in whole or in part, the CE must: 1) to the extent possible, give the individual access to any other requested (and releasable) PHI, after excluding the PHI that the CE has a ground to deny; and, 2) provide a timely, written response that contains the basis for the denial, a statement of the individual's right to request review how the individual may exercise the review rights, if applicable, and how the individual may complain to the CE or to HHS.

RIGHT TO REQUEST AN AMENDMENT

Individuals have the right to request an amendment to their PHI maintained in a designated record set. A CE may require individuals to make requests in writing and to provide a reason for the requested amendment, if the CE informs the individuals in advance. The CE must respond within 60 days and is permitted one 30-day extension, if the individual is notified of the reason for the delay and the date the CE will complete its action on the request. If the request is accepted, the CE must make the amendment to the PHI or record by, at a minimum, identifying the records in the designated record set that are affected and appending or otherwise providing a link to the location of the amendment. The CE must also make reasonable efforts to inform others who the individual identifies as needing the amendment and who the CE knows has the PHI and has relied or may rely on the information to the detriment of the individual.

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 explaining the individual's right to file a written statement of disagreement. DoD 6025.18-R, Chapter 12, provides information on the process and procedures to be followed by a DoD CE receiving such a request.

RIGHT TO AN ACCOUNTING OF DISCLOSURES

Individuals have a right to receive an accounting of disclosures of their PHI made by a CE and its BAs, in the six years prior to the date of the request. However, a CE is not required to account for disclosures of PHI under the following circumstances:

- To carry out TPO
- To individuals about their PHI
- Pursuant to the individual's written and signed authorization
- For the facility's directory, to persons involved in the individual's care, or for 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
- Incident to permitted uses or disclosures
- As part of a limited data set
- That occurred prior to the compliance date

CEs must respond within 60 days of the request by providing the individual with the accounting requested. If the CE is unable to provide the accounting within the 60 days, a CE may have one 30-day extension to provide the accounting, if it provides the individual with a written statement of the reasons for the delay and the date the CE will provide the accounting. DoD 6025.18-R, Chapter 13, provides guidance and specific requirements on how to respond to a request for accounting of disclosures.

Individuals are entitled to one no cost accounting of disclosures in a 12-month period, but a CE may charge a reasonable cost-based fee for additional requests in the same 12-month period, with prior notice to the individual of charges.



RIGHT TO FILE A COMPLAINT

Individuals have the right to file a complaint directly with a military treatment facility (MTF) HIPAA Privacy Office, the DHA Privacy Office, and/or the HHS Office for Civil Rights, if they feel a CE has committed a violation of the HIPAA Privacy, Security, or Breach Notification Rules. Under the HIPAA Privacy Rule, a CE must provide a process for individuals to make complaints concerning the CE's policies and procedures. See DoD 6025.18-R, paragraph 14.4.

i MHS NoPP

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

CUSTODIAL AND NONCUSTODIAL PARENTS

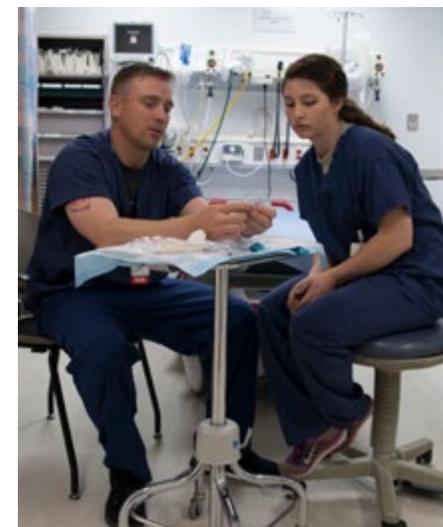
Subject to limitations under applicable State law, a minor's PHI may be released to either parent, unless the CE is provided legal documentation potentially affecting parental authority with respect to the minor's health care. In that situation, the CE should review the documentation to verify which parent has authority with respect to the minor's health care and whether disclosure of the minor's PHI to either parent is restricted. DoD 6025.18-R, paragraph C8.7, sets forth how DoD CEs determine who is the personal representative of an unemancipated minor, an adult, and an emancipated minor under applicable law.

i NEW RESOURCE

The DHA HIPAA Privacy Rule Web Assessment Tool is a comprehensive web-based instrument to aid MTFs in assessing their compliance with the HIPAA Privacy Rule. Upon responding to a series of questions, the user will receive a customized assessment report identifying opportunities to enhance or develop HIPAA Privacy Rule related policies and procedures and highlighting resources and best practices to improve MTF HIPAA Privacy Rule compliance. User responses will not be accessed or viewed by the DHA Privacy Office.

INTERCONNECTEDNESS

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



LOOKING AHEAD

DoD 6025.18-R, DoD Health Information Privacy Regulation, which implements the HIPAA Privacy Rule within the MHS, is currently under revision. Upon publication of the updated guidance, the DHA Privacy Office will release a mapping between DoD 6025.18-R and the DoDM 6025.18 to help familiarize stakeholders with the updated content and organization.

One significant change is the designation of DoD as a hybrid entity. Due to a lack of clarity when HIPAA was enacted as to whether affiliated CEs could designate themselves as a hybrid entity, DoD designated itself as a single affiliated CE in DoD 6025.18-R. On the surface, this would suggest that all DoD components are regulated by HIPAA. However, DoD functionally structured itself as a hybrid entity. In a hybrid entity, only the organization's covered components and BAs of covered components are required to comply with HIPAA. DoD's covered components include components functioning as health plans and healthcare providers that conduct standard electronic transactions. By limiting the application of HIPAA, DoD, as a hybrid entity, can reduce unnecessary exposure to administrative obligations, legal risks, and unintended costs. Until the new guidance is issued, the DHA Privacy Office, in collaboration with DHA's Office of General Counsel, has issued an Information Paper clarifying DoD's structure under HIPAA as a hybrid entity. The Information Paper entitled, *DoD's Structure under HIPAA and its Impact on Various DoD Components*, is available at <https://health.mil/Reference-Center/Publications/2017/04/19/DoDs-Structure-under-HIPAA-and-its-Impact-on-Variou-DoD-Components>.

Other notable changes include:

- Adoption of a new provision directing CEs that disagree with a PHI request by a military command authority to seek the advice of the cognizant HIPAA Privacy Officer or legal counsel prior to making a disclosure determination
- Incorporation of DoDI 6490.08, Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members, which lays out the standards governing the notification of military command authorities when an Armed Forces member obtains mental health services or substance abuse education services
- Implementation of a new requirement that CEs must verify the identity and authority of any person or entity requesting PHI, if the identity or such authority is not known to the CE
- Incorporation of the requirement that a CE's workforce members must follow established policies and procedures when seeking to exercise their individual rights
- Clarification that audit logs or access reports, which provide information on who has accessed PHI, are not part of a designated record set



POINTS OF CONTACT

DHA.PrivacyMail@mail.mil for HIPAA Privacy-related questions

DHA.PrivacyMaterials@mail.mil for DHA Privacy Office materials

RESOURCES

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

DoD Health Information Privacy Regulation
 DoD 6025.18-R, January 24, 2003
 (currently under revision)

HIPAA Privacy Rule
 45 Code of Federal Regulations Parts 160 and 164

HIPAA Privacy Rule Web Assessment Tool
 (requires Common Access Card to access)
https://info.health.mil/cos/admin/privacy/SitePages/HIPAA_Tool.aspx

HIPAA SECURITY

Putting HIPAA Security Safeguards to Work

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

WHO IS COVERED?

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



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

i HIPAA SECURITY RISK ASSESSMENT

As part of its Risk Management Program, the DHA Privacy Office annually conducts an internal HIPAA Security Risk Assessment (HSRA) in accordance with Department of Defense Instruction (DoDI) 8580.02, *Security of Individually Identifiable Health Information in DoD Health Care Programs*. The HSRA evaluates the security safeguards found in DoDI 8580.02 while considering the security controls that are evaluated through the DHA Risk Management Framework (RMF) Assessment and Authorization (A&A) process based on DoDI 8510.01, *Risk Management Framework in DoD Information Technology (IT)*, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

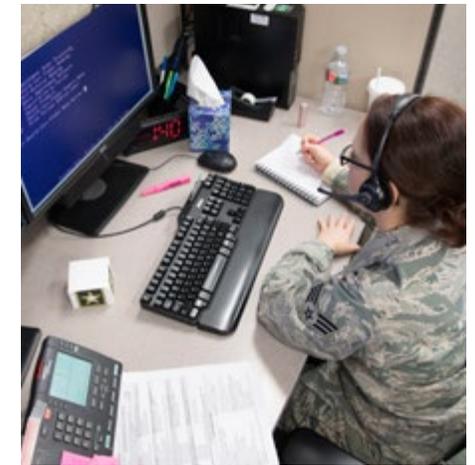
RISK MANAGEMENT AND THE HIPAA SECURITY RULE

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

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

To assist HIPAA Security Officers in assessing reasonable and appropriate safeguards, the Privacy Overlays have been developed to identify minimum protections for ePHI. The Privacy Overlays

link security controls from the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, to each HIPAA Security Rule standard and implementation specification.²



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

As organizations conduct HIPAA risk assessments, they may find that more stringent controls are appropriate than those that have been identified in the Privacy Overlays. Nothing in the Privacy Overlays prohibits organizations from applying more stringent controls to safeguard ePHI based on the results of their risk analysis. Conversely, the risk analysis may identify certain controls that are not applicable. For example, a system that merely stores appointment information will still fall under the protection of HIPAA, but may not need the same set of security and privacy controls that would be appropriate for an electronic health records system. Organizations should seek legal counsel if they are considering tailoring or otherwise altering the security and privacy controls identified in the Privacy Overlays.

i KEY ELEMENTS OF RISK ANALYSIS

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



THE HIPAA SECURITY RULE SAFEGUARDS

Administrative safeguards are designed to protect ePHI and to manage the conduct of DoD CEs' workforce using ePHI in the performance of their jobs. There are nine administrative safeguards identified in DoDI 8580.02:

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

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

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

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

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

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

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

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



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

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

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

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

Access Controls carry out the implementation of the Information Access Management standard, which set the rules on which workforce members can and should have access to the different types of data, how much data they should access (in accordance with the Minimum Necessary Rule), and what privileges they should have (read, write, etc.) in order to perform job functions. Because electronically stored information can be lost, stolen, damaged, or destroyed if stored improperly or when equipment is moved, implementation specification for Data Backup and Storage requires that DoD CEs “create retrievable, exact copies of ePHI, when needed, before movement of equipment.”

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

i STOP AND THINK – DATA PROTECTION 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
- ✓ Always encrypt e-mails that contain personally identifiable information (PII) and PHI

globe INTERCONNECTEDNESS

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




LOOKING AHEAD
DHA Privacy Office RMF Process Integration

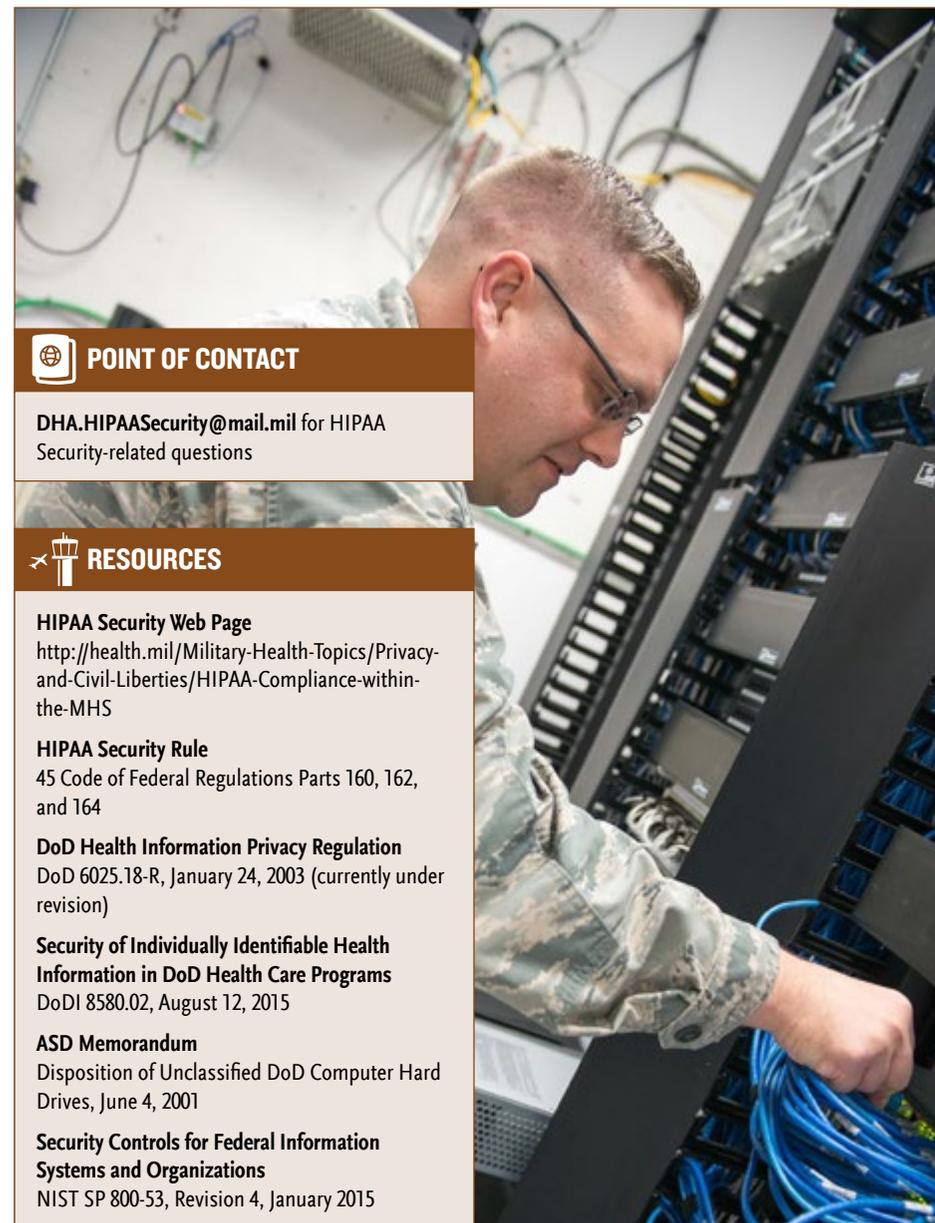
The Office of Management and Budget (OMB) Circular A-130 along with a fully implemented RMF process require that, for the first time, all government Privacy Offices become a part of the Information System A&A approval process. The DHA Privacy Office was proactive in understanding the impact of these mandated changes on DHA's overall RMF workflow and the potential impact that would be placed on organizational Information System Owners.

As a result, the DHA Privacy Office advocated for and established an inter-organization Privacy-RMF working group between the DHA Privacy Office and DHA Health Information Technology (HIT) Cyber Security Division (CSD) A&A in an effort to develop, integrate, and implement new processes and guidance documents pertinent to the overall authority to operate (ATO) process. This workgroup, comprised of privacy, legal, cybersecurity, and policy subject matter experts from within the DHA Privacy Office, reviewed the existing DHA RMF process and provided expert guidance and revision to the DHA RMF workflow by going through the systematic process, step-by-step, and augmenting the implementation guidance with updated detailed privacy instructions and privacy review gates for improved regulatory compliance.

The joint Privacy-RMF Workgroup also performed the much-needed analysis on 204 identified privacy-specific DoD Control Correlation Identifiers (CCI) in an effort to provide a privacy-centric contextual mapping for its implementation as required per the DoD RMF Technical Advisory Group (RMF-TAG). This updated guidance will enable both DoD and DHA Information System Owners to implement the privacy controls as required per DoD regulation and OMB directive.

The DHA Privacy Office's work will significantly enhance DHA Information System Owners' ability to better inherit identified Common Controls as implemented through the DHA enterprise Enterprise Mission Assurance Support System tool per DoD and Committee on National Security Systems 1253. As a result, reliance can now be had on the 200+ privacy artifacts specific to the DHA Tier 2 System of Record (T2SOR) to meet the "compelling evidence" requirements. The development of this T2SOR will make it more efficient for hundreds of information systems that manage or process PII going through the A&A process to more readily obtain their ATO. The 170 specific DHA Implementation Guidance for Information System Owners, Information System Security Managers, and DHA HIT CSD A&A Assessors can be used to better interpret the required Appendix J privacy controls/CCIs, and to improve their chances to more effectively conform their information system to approved DHA risk acceptance levels and enhancement of the overall RMF ATO process.

Documentation developed to date includes the Privacy Program Plan which also serves as a Concept of Operations for the DHA Privacy Office and the System Privacy Plan, which provides detailed information on the privacy profile of an Information System and is an essential documentation requirement within the RMF approval process. The Privacy Continuous Monitoring Strategy, PII Confidentiality Impact Level methodology, and the Privacy Assessment Methodologies and Metrics are currently under development. The DHA Privacy Office will provide ongoing support and privacy subject matter expertise as necessary within the RMF process including evaluation of privacy risk for systems undergoing the ATO process, training, compelling evidence updates, and revised interpretations based on clarifications published by oversight bodies.



POINT OF CONTACT

DHA.HIPAAsecurity@mail.mil for HIPAA Security-related questions


RESOURCES
HIPAA Security Web Page

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

HIPAA Security Rule

45 Code of Federal Regulations Parts 160, 162, and 164

DoD Health Information Privacy Regulation

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

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoDI 8580.02, August 12, 2015

ASD Memorandum

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

Security Controls for Federal Information Systems and Organizations

NIST SP 800-53, Revision 4, January 2015

HIPAA TRANSACTIONS, CODE SETS, AND IDENTIFIERS

HIPAA Compliance

The HIPAA Administrative Simplification provisions require the Department of Health and Human Services to establish national standards for electronic healthcare transactions, code sets, and identifiers (TCS&I). National standards for HIPAA TCS&I improve the effectiveness and efficiency of the healthcare industry by requiring a level of healthcare industry-wide commonality when it comes to the electronic transmission of certain healthcare administrative information.

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



WHICH HIPAA CEs NEED TO COMPLY?

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

- Providers (e.g., military treatment facilities, civilian hospitals, civilian clinics), individuals (e.g., physicians, nurse practitioners, physician assistants), and group provider practices
- Health plans (e.g., TRICARE, Blue Cross/Blue Shield®)
- Clearinghouses (e.g., ePremise®, Emdeon®)
- Business associates of the CEs (e.g., Defense Manpower Data Center/Defense Enrollment Eligibility Reporting System (DMDC/DEERS), TRICARE Regional Contractors)



INTERCONNECTEDNESS

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

- Coding as related to certain code sets used in HIPAA transactions
- Access to Care as related to eligibility, enrollment, and referral transactions and processes
- TRICARE Private Sector Care as related to the insertion of HIPAA TCS&I requirements language into TRICARE manuals as appropriate
- Human Resources as related to implementation, availability, and use of National Provider Identifier (NPI) in HIPAA transactions, etc.
- Collaboration with other federal agencies, healthcare industry organizations, Service Medical Department points of contact, and other DHA offices
- Defense Medical Logistics as related to implementation and use of Unique Device Identifiers for medical devices



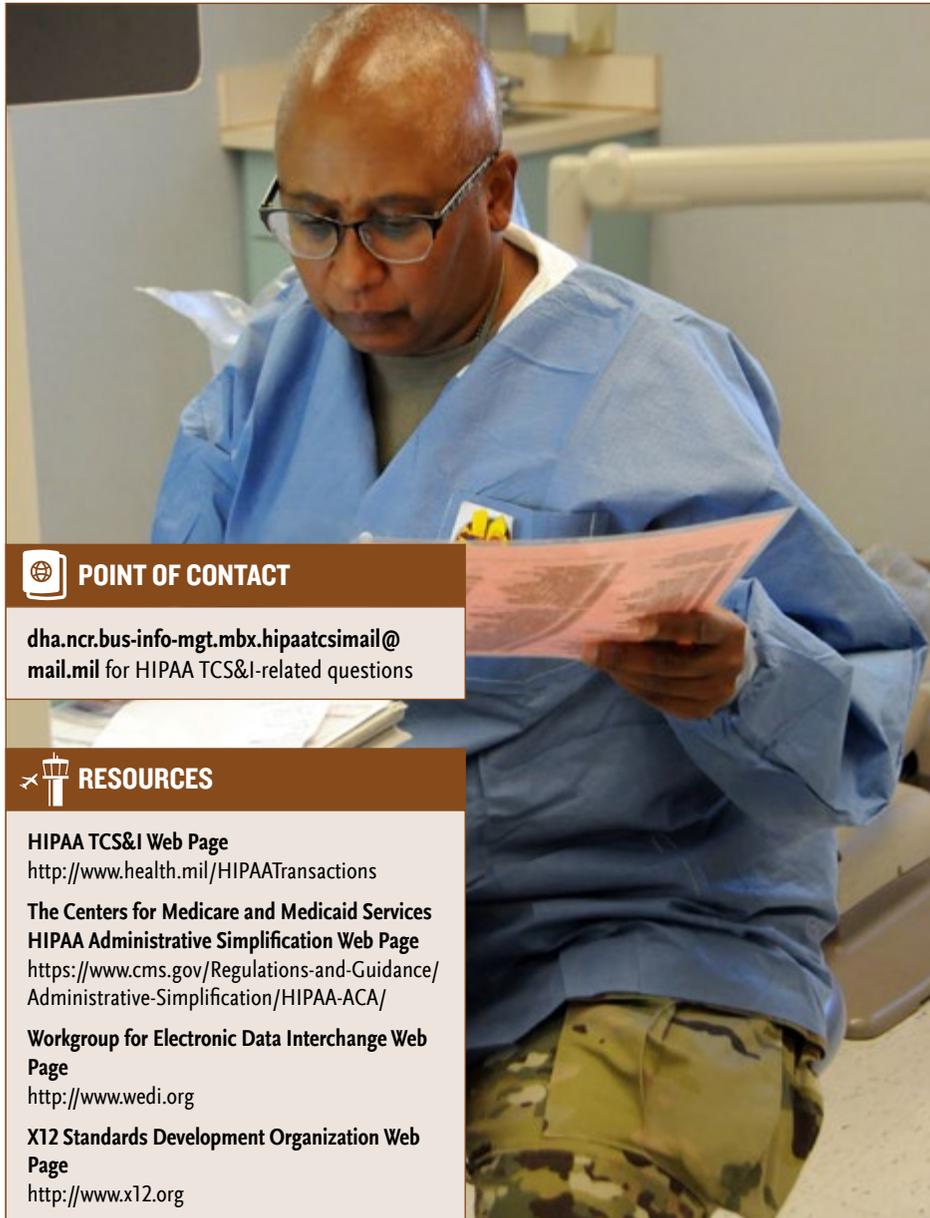
LOOKING AHEAD

The HIPAA TCS&I Program is preparing for upcoming HIPAA initiatives including Health Plan Certification of Compliance with HIPAA-mandated transaction standards and Operating Rules, Clinical Attachments for referral and claims transactions, and implementation of the next mandated version of the national standards for electronic healthcare transactions (expected to be X12 version 7030, as well as National Council on Prescription Drug Programs version F2).

HIPAA-mandated identifiers have included the Employer Identifier, the NPI, and the Health Plan Identifier (HPID), though HPID was never fully implemented. These identifiers are intended to be used as data within HIPAA transactions and may also be used for other non-HIPAA purposes.

HIPAA also mandates the use of certain code sets within HIPAA adopted transactions. For example, ICD-10 (the International Classification of Diseases, 10th Revision, Clinical Modification (CM) and Procedure Coding System (PCS)) are code sets required by HIPAA. HIPAA-mandated code sets may also be used for non-HIPAA purposes.





POINT OF CONTACT

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

RESOURCES

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

**The Centers for Medicare and Medicaid Services
 HIPAA Administrative Simplification Web Page**
[https://www.cms.gov/Regulations-and-Guidance/
 Administrative-Simplification/HIPAA-ACA/](https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/)

**Workgroup for Electronic Data Interchange Web
 Page**
<http://www.wedi.org>

**X12 Standards Development Organization Web
 Page**
<http://www.x12.org>

PRIVACY AND RISK MANAGEMENT

Integrating Security Standards

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

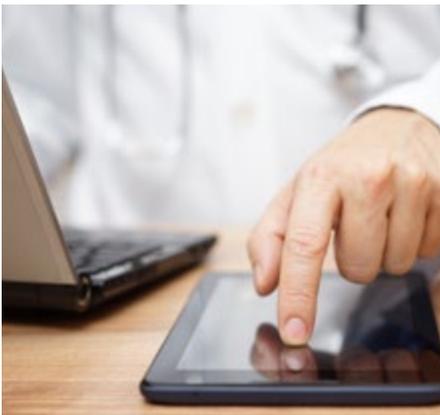
The DHA Privacy Office participated in an effort to further develop the necessary specific guidance for electronic protected health information (ePHI) on its transition through the Committee on National Security Systems Privacy Overlays Working Group. This working group is one of several government working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

The Privacy Overlays are a specification of privacy-centric security controls, that include supporting guidance used to complement the security control baseline selection according to DoD policy, and the supplemental guidance found within the NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. They are used as a tool by information systems security engineers, authorizing officials, privacy officials, and others to select appropriate protections for differing privacy information types, including ePHI.



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

Most notably, the Privacy Overlays allow privacy officials and cybersecurity experts the ability to align existing security and privacy requirements applicable to a specific computing system containing ePHI or PII. The use of the Privacy Overlays alongside NIST security control baselines allows for security and privacy controls to be customizable and implemented as part of an organization-wide process that manages cybersecurity and overall privacy risk.



i PRIVACY OVERLAYS FRAMEWORK

- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- Committee on National Security Systems Instruction (CNSSI) No. 1253, March 27, 2014
- Privacy Act of 1974, as amended (5 United States Code 552a)
- E-Government Act of 2002 (Public Law 107-347)

HOW DOES IT WORK?

Not all PII must be protected equally. NIST SP 800-122, *Guide to Protecting the Confidentiality of PII*, provides a methodology to both categorize PII and determine the PII confidentiality impact level – low, moderate, or high. Based on the sensitivity of PII in the system, the methodology indicates the potential harm that could result if PII was inappropriately accessed, used, or disclosed.

The PII confidentiality impact level is used to determine which security and privacy controls apply to a given system. While this may appear similar to the impact values for the security objectives of a system (confidentiality, integrity, and availability), it is very different. The system security objectives are used to determine the security control baselines in CNSSI No. 1253. Protected health information (PHI) is a subset of PII that comes with a distinct set of applicable laws and regulations. In addition to those that apply to all types of PII, the Privacy Overlays distinguish between PII and PHI to clearly document the supplemental guidance, control extensions, and regulatory and statutory references that apply specifically to PHI (e.g., the HIPAA Privacy and Security Rules).¹

By definition, PHI is PII; thus, the laws, regulations, and other standards for safeguarding PII also apply to PHI. Therefore, the organization must follow the guidance contained in the Privacy Overlays to determine the PII confidentiality impact level of the information it owns or manages and apply the appropriate subpart of the Privacy Overlays (e.g., low, moderate, or high). After determining the PII confidentiality impact level, the organization must also consider the guidance related to PHI within the Privacy Overlays.

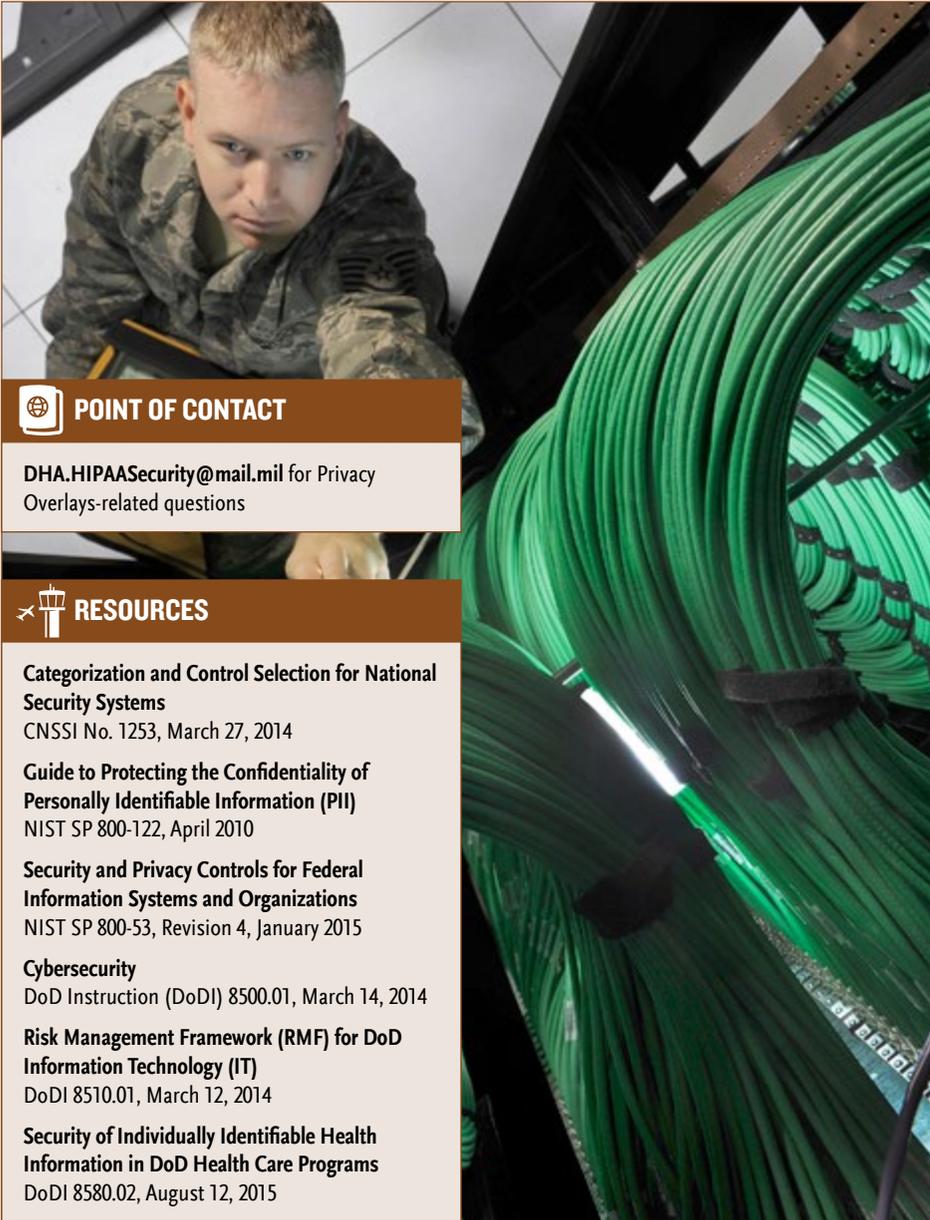
¹ The PHI subpart of the Privacy Overlays applies to all federal government agencies that adopt CNSSI No. 1253 and are covered entities or business associates.

globe INTERCONNECTEDNESS

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

hand LOOKING AHEAD

The Privacy Overlays are currently being tailored and extended further to address other "special topics" (e.g., cloud, mobile, wearables). As of March 6, 2017, DoD has released *Cloud Computing Security Requirements Guide* Version 1, Release 3 with explicit guidance to Mission Owners on the use of cloud system/application intending to store and process PII and/or PHI.



POINT OF CONTACT

DHA.HIPAAsecurity@mail.mil for Privacy
Overlays-related questions

RESOURCES

Categorization and Control Selection for National Security Systems

CNSSI No. 1253, March 27, 2014

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

NIST SP 800-122, April 2010

Security and Privacy Controls for Federal Information Systems and Organizations

NIST SP 800-53, Revision 4, January 2015

Cybersecurity

DoD Instruction (DoDI) 8500.01, March 14, 2014

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

DoDI 8510.01, March 12, 2014

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoDI 8580.02, August 12, 2015

DATA SHARING

Requesting DHA Data

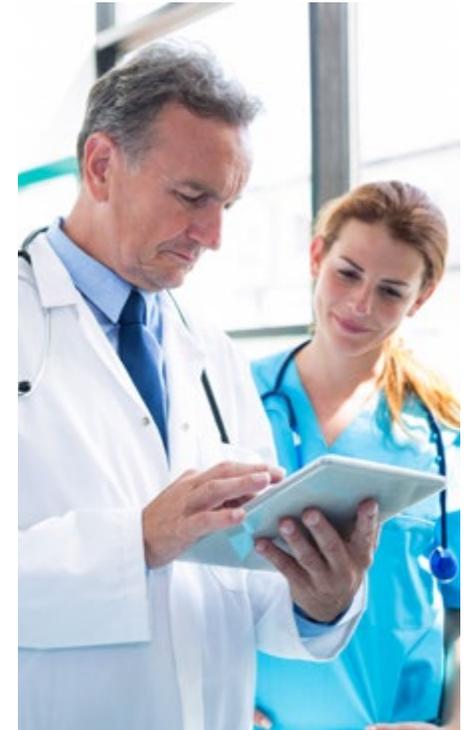
The DHA Privacy Office receives various types of data sharing requests for DHA data. Under its Data Sharing Program, the DHA Privacy Office reviews each request for compliance with applicable privacy and security regulatory requirements.

The DHA Privacy Office neither grants system access nor provides data extractions; however, prior to gaining access to receiving an extraction of data, program offices require an executed Data Sharing Agreement (DSA). 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.

DSA PROGRAM

The DSA Program was established within the DHA Privacy Office to carry out the following:

- Confirm whether a requested use or disclosure of DHA data is permitted or required by applicable DoD privacy and security regulations and policies
- Promote privacy compliance
- Maintain DSA documentation in the case of an investigation or audit
- Establish compliance checks to:
 - Make reasonable efforts when disclosing data to limit the information to the minimum necessary for achieving the intended purpose
 - Abide by information protection regulations



DATA SHARING AGREEMENT APPLICATION (DSAA)

Before a DSA is executed, the DHA Privacy Office uses a DSAA to accomplish the following objectives:

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

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

- The requested data adheres to applicable System of Records Notice requirements
- The information system(s) and networks intended for processing and/or storing the requested data have appropriate physical, administrative, and technical safeguards
- Research-related data use requests have been reviewed by the appropriate compliance offices and obtained the related determinations, including the Institutional Review Board (IRB), the DHA Human Research Protection Program (HRPP), and the DHA Privacy Board

i A DSAA MUST BE INITIATED BY THE FOLLOWING:

Applicant – The individual who provides oversight and responsibility for the data.

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

Government Sponsor – The point of contact within DHA or the respective Armed Service who assumes responsibility for the contract, grant, project, or Cooperative Research and Development Agreement. This role can be filled by a civilian within DHA or a uniformed Service member.

Once all compliance reviews are completed and the DHA Privacy Office approves the DSAA, 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, excluding protected health information (PHI)
- DSA for limited data set, known as a Data Use Agreement
- DSA for PHI

DHA PRIVACY BOARD

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

There are four types of DHA Privacy Board reviews:

1. Studies that must obtain HIPAA authorizations from each participant. The DHA Privacy Board will review the proposed authorization for HIPAA compliance
2. Studies that require an Application for a Waiver of Authorization or Altered Authorizations. Waivers are required when it is not possible or practicable to get authorizations from all study participants. Altered Authorizations are required for studies where it is not possible to include all of the core elements and required statements. HIPAA requires researchers to include in authorizations
3. Studies that are solely conducted on the PHI of decedents (no live subjects) must submit Required Representations for Research on Decedents' Information
4. Studies that require access to or use of PHI solely for preparing a research protocol, identifying potential research participants, or similar pre-study activity must submit Required Representations for Review Preparatory to Research. This cannot be used if the researcher plans to remove PHI from the MHS or to contact individuals during these pre-study activities

RESEARCH DATA SHARING STREAMLINING INITIATIVE

The DHA Privacy Office has implemented initiatives to help streamline the separate and distinct reviews required by the Federal Policy for Protection of Human Subjects (also known as the “Common Rule”) and the HIPAA Privacy Rule, so that a single board can simultaneously conduct both reviews. On April 1, 2016, DHA officially delegated regulatory reviews of research-related data sharing requests to the DHA's National Capital Region Medical Directorate Military Treatment Facilities, including Walter Reed National Military Medical Center and Fort Belvoir Community Hospital.

The DHA Privacy Office also expanded its outreach efforts within the MHS, providing training to IRB members and other research oversight staff on HIPAA Privacy Rule requirements and on standardized templates that should be used to perform HIPAA Privacy Rule reviews of research studies. In response to the high level of training requests in this regard, the DHA Privacy Office recently launched an online training course on Joint Knowledge Online, listed in the course catalog as “DHA-US096: HIPAA Privacy Rule Compliance Training for Institutional Review Boards and HIPAA Privacy Boards.”



ARE YOU READY TO SUBMIT YOUR REQUEST?

- ✓ Have you completed the online DSAA?
- ✓ Have you adequately described the process to receive, use, de-identify, store, publish, and/or report the data?
- ✓ Do you have all applicable compliance approvals required for this data use and disclosure?
- ✓ Have you provided a clear purpose for the data requested?
- ✓ Have you included the appropriate Data Request Template?
- ✓ Did both the Applicant and Government Sponsor initial the request?

INTERCONNECTEDNESS

In the process of reviewing a DSAA, prerequisite reviews and approvals may be identified. These may include IRB approval, HRPP determination, Data Evaluation Workgroup review, DHA Privacy Board review, Service level approval, or System Security Verification review and approval. DSAs are analyzed to ensure that business associates have a Business Associate Agreement in their contract. The DSA Program supports both program offices and Data Managers through its DSAA reviews.

LOOKING AHEAD

- The DHA Privacy Office continues to monitor as more systems and organizations become part of the DHA
- Updated standard HIPAA research templates will ultimately be available on electronic IRB (eIRB) for easy-access by all researchers and IRBs
- Annual DSA Reports are available after the close of each fiscal year
- Annual DHA Privacy Board Reports are available online after the close of each fiscal year



POINTS OF CONTACT

DHA.DataSharing@mail.mil for DSA-related questions

DHA.PrivacyBoard@mail.mil for DHA Privacy Board, Streamlining Initiative, and MHS data expert-related questions

DHA.PrivacyMail@mail.mil for HIPAA Privacy-related questions

RESOURCES

DSA Web Page

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

DHA Privacy Board Web Page

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

DoD Health Information Privacy Regulation

DoD 6025.18-R, DoD Health Information Privacy Regulation, January 24, 2003 (currently under revision)

Security of Individually Identifiable Health Information in DoD Health Care Programs

DoD Instruction 8580.02, August 12, 2015

HUMAN RESEARCH PROTECTION PROGRAM

Research Compliance

DoD supports and encourages research, including human subject research, to continue to improve and enhance medical science and health care for all MHS beneficiaries. All research protocols that include human subjects must be compliant with federal laws, federal regulations, and DoD policies intended to protect the voluntary subjects of the studies. The Department of Health and Human Services (HHS) published the original rule protecting human subjects in research, *The Federal Policy for the Protection of Human Subjects*, known as the “Common Rule.” This rule was adopted within DoD in Part 219 of Title 32 Code of Federal Regulations (CFR). The DoD policy implementation of the Common Rule is DoD Instruction (DoDI) 3216.02, *Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research*. In January 2017, HHS published an updated, modernized version of the Common Rule to improve efficiency in research and to enhance protections of human subjects. The DoD is currently working to revise policies to incorporate the provisions of the final Common Rule.

The DHA Human Research Protection Program (HRPP) ensures that research is conducted in accordance with these applicable rules and ethical guidelines that serve to protect the rights and welfare of participants, Service members, employees, and their families.

HRPP COMPLIANCE REVIEWS

DoD Institutional Review Boards (IRBs) provide HRPP compliance reviews. Within the DHA, Walter Reed National Military Medical Center has multiple IRBs that provide compliance reviews of research studies that originate within the Office of the Assistant Secretary of Defense (Health Affairs) or DHA.

HRPP COMPLIANCE REVIEWS

All documents for HRPP compliance reviews must be submitted using the Electronic Institutional Review Board (eIRB) at <https://dmrncac.dhhq.health.mil>.

For questions regarding the HRPP or for information on using the eIRB, please send an e-mail message addressed to DHA.HRPP@mail.mil.

DoD IRBs conduct HRPP reviews to ensure compliance with:

- 32 CFR Part 219, *Protection of Human Subjects* (DoD’s adoption of the Common Rule)
- Food and Drug Administration Regulation, 21 CFR Parts 50, 312, 600 and 812
- HHS Regulation, *Protection of Human Subjects*, 45 CFR Part 46, Subparts B, C, and D (Common Rule)
- 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*

Studies that are approved by non-DoD IRBs with federal-wide assurance from HHS require subsequent review by the DoD HRPP to ensure compliance with DoD specific requirements. Non-DoD institutions must also attest to their understanding of and adherence to DoD-specific protections.

Defense Health Headquarters HRPP reviews include the following:

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



For research studies that do not require review by an IRB, the DHA HRPP Office conducts the following reviews and consultative services:

- Human subject and/or research determination
- Exemption determination
- Human Research Protection Official's review
- Protocol modification review
- Continuing review

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



INTERCONNECTEDNESS

Before a research Data Sharing Agreement (DSA) can be executed, it must be determined that the project is compliant with the ethical standards for the protection of human subjects. Consequently, the DHA HRPP is tightly integrated with the DHA DSA Program. In addition, the DHA HRPP works with the DHA Privacy Board in reviewing research studies requiring protected health information for compliance with the HIPAA Privacy Rule.



LOOKING AHEAD

On January 19, 2017, HHS released the final revisions of the Common Rule to go into effect in January 2018 (2018 Requirements). However, on January 17, 2018, HHS announced a six-month delay of the 2018 Requirements and published an interim final rule that delays the effective date and general compliance date of the 2018 Requirements to July 19, 2018. The federal departments and agencies listed in the interim final rule are in the process of developing a proposed rule to further delay the implementation of the 2018 Requirements to January 2019. The reason for the interim final rule is to provide time to both implement the 2018 Requirements as well as seek input from stakeholders on further delaying the implementation of the 2018 Requirements.





POINT OF CONTACT

DHA.HRPP@mail.mil for HRPP-related questions

RESOURCES

HRPP Web Site

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

Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research
DoDI 3216.02, November 8, 2011

BREACH RESPONSE

Prevention and Mitigation

Preparation is critical for an effective Privacy Compliance Program. When faced with a breach as defined by the Privacy Act of 1974 and/or the HIPAA Breach Notification Rule, having a clear understanding of what breaches are, why they occur, and how to prevent them is key to compliance. Mishandled or misused personally identifiable information (PII) or protected health information (PHI) can result in a breach or HIPAA Privacy violation. This chapter is designed to serve as a quick reference on how to prevent breaches and how to mitigate breaches, if they occur.

WHAT IS A BREACH?

Under the Privacy Act and as defined by DoD, a breach is “a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations, where persons other than authorized users and for an other than authorized purpose, have access or potential access to PII, whether physical or electronic.”

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



BREACH REPORTING

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

FOR DHA	FOR SERVICE COMPONENTS
LEADERSHIP: Immediately	LEADERSHIP: Immediately
US COMPUTER EMERGENCY READINESS TEAM (US-CERT): Within 1 hour of a confirmed cyber security incident*	US-CERT: Within 1 hour of a confirmed cyber security incident*
DHA PRIVACY & CIVIL LIBERTIES OFFICE: Within 1 hour of discovery	DoD COMPONENT SENIOR PRIVACY OFFICIALS: Within 24 hours of discovery
DEFENSE PRIVACY, CIVIL LIBERTIES, & TRANSPARENCY DIVISION (DPCLTD): Within 48 hours**	DHA PRIVACY & CIVIL LIBERTIES OFFICE: Within 24 hours of discovery
DEPARTMENT OF HEALTH AND HUMAN SERVICES:** <ul style="list-style-type: none"> • Within 60 days of discovery if 500 or more individuals are impacted • Within 60 days of the close of the calendar year if less than 500 individuals are impacted 	DPCLTD: Within 48 hours***
<p>* US-CERT reporting is no longer required for non-cyber related incidents (e.g., breaches involving paper records, unauthorized verbal disclosures).</p> <p>** DHA is responsible for reporting to DPCLTD and the Secretary of HHS.</p> <p>*** The Service Components are responsible for reporting up their chain of command and to DPCLTD.</p> <p><i>NOTE: If necessary, notify issuing banks (if government issued credit cards are involved); law enforcement; and all affected individuals within 10 working days of breach discovery and the identities of the impacted individuals that have been ascertained. Contact your designated DoD Senior Privacy Official or the DHA Privacy Office for additional guidance.</i></p>	

i US-CERT REPORTING REQUIREMENTS

In accordance with the Department of Homeland Security's *US-CERT Federal Incident Notification Guidelines*, dated January 14, 2015, all federal agencies are required to only report confirmed cyber related incidents to US-CERT within one hour. Non-cyber related breaches (e.g., breaches involving paper records or other non-digital/electronic information) are not required to be reported to US-CERT.

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

i BREACH PREVENTION TIPS

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

THE SEVEN STEPS TO AN EFFECTIVE BREACH RESPONSE PLAN

1. BREACH IDENTIFICATION

Recognize that an event has occurred and initiate next step

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

2. BREACH REPORTING

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

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

3. CONTAINMENT

Limit the impact of the breach

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

4. MITIGATION

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

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

5. ERADICATION

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

- Deleting any computer viruses
- Updating beneficiary contact information

6. RECOVERY

Restore business operations to normal status

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

7. FOLLOW-UP

Take necessary actions to prevent future occurrences

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

BREACH POLICIES AND PROCEDURES

Policies and procedures necessary for an effective breach response management plan include:

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

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

COMPLIANCE ENFORCEMENT

Enforcement of sanctions for compliance violations is vital to breach prevention. The implications of compliance violations – for individuals and the organization – should be reviewed with staff members regularly. Ensuring consequences are imposed for breaches of PII/PHI will encourage staff members to take compliance seriously. Therefore, the following tips are recommended:

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

DHA ADMINISTRATIVE INSTRUCTION (AI) 71

Incident Response Team (IRT) and Breach Response Requirements

Re-signed on September 15, 2015, this AI outlines the processes and procedures for assessing and responding to confirmed or suspected breaches occurring within DHA. Responsible individuals and supervisors should follow these guidelines when a breach or suspected breach occurs. The AI also continues the requirement for the IRT to convene annually for training purposes. This year's IRT exercise was held on March 20, 2018 and continued on May 8, 2018 (due to inclement weather), at the Defense Health Headquarters.

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

WORKFORCE TRAINING

Prioritizing staff training and improving its effectiveness are essential to ensure compliance with the appropriate privacy and security policies. Therefore, the following tips are recommended:

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



INTERCONNECTEDNESS

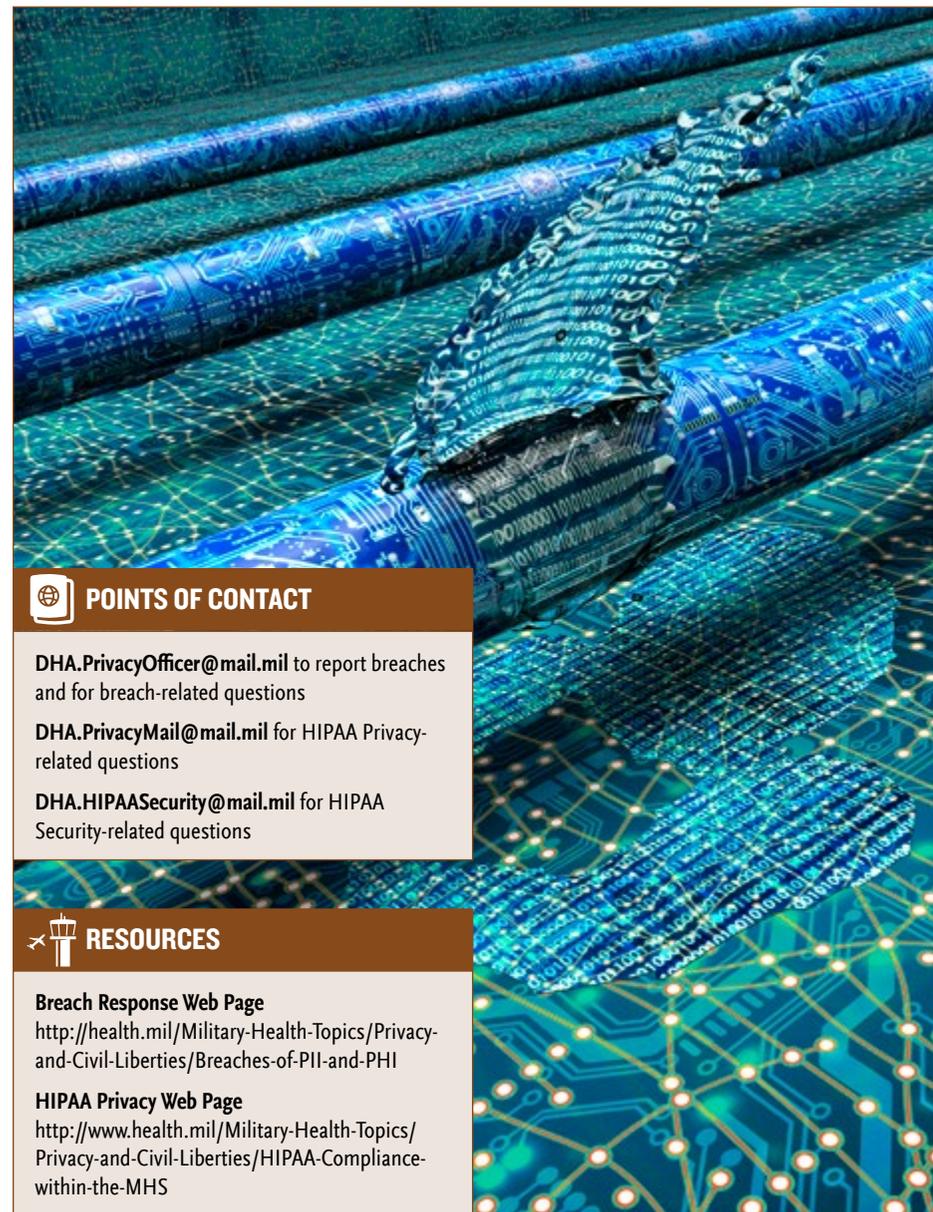
An effective breach response plan is key to an agency's preparedness; however, in order to respond to a breach correctly, a breach needs to be analyzed under Privacy Act requirements, and HIPAA Breach Notification Rule requirements may also need to be considered.

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



LOOKING AHEAD

Revisions to DoD's implementation of the HIPAA Privacy Rule remain in coordination. For the first time, this DoD issuance will include HIPAA breach reporting requirements for the MHS in accordance with the HIPAA Breach Notification Rule.



POINTS OF CONTACT

DHA.PrivacyOfficer@mail.mil to report breaches and for breach-related questions

DHA.PrivacyMail@mail.mil for HIPAA Privacy-related questions

DHA.HIPAASecurity@mail.mil for HIPAA Security-related questions



RESOURCES

Breach Response Web Page

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

HIPAA Privacy Web Page

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

MILITARY COMMAND EXCEPTION

Disclosing Protected Health Information (PHI) of Armed Forces Personnel

In accordance with the HIPAA Privacy Rule, DoD 6025.18-R, DoD Health Information Privacy Regulation, January 24, 2003 and applicable DoD issuances, a DoD covered entity (CE) may use and disclose the PHI of individuals who are Armed Forces members for activities deemed “necessary by appropriate military command authorities to assure the proper execution of the military mission.” This is commonly referred to as the “Military Command Exception.” See paragraph C7.II.1.2 of the DoD 6025.18-R for information on “appropriate military command authorities.”

This exception explains when DoD providers may: 1) disclose Service members’ PHI to military commanders or 2) use Service members’ PHI for military commanders’ purposes, such as evaluating

fitness for duty. If the specific requirements of this exception are satisfied, patient authorization is not required for such uses or disclosures. Note that disclosures of PHI under the military command exception are permitted; they are not required. Although non-DoD CEs are not required to abide by DoD 6025.18-R, the exception is still applicable to private hospitals and physicians as it is stated in the HIPAA Privacy Rule at 45 Code of Federal Regulations (CFR) 164.512(k)(1)(i).

i ARMED FORCES PERSONNEL

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

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

i MILITARY COMMAND AUTHORITY

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

MILITARY COMMAND AUTHORITIES

Appropriate military command authorities include commanders who exercise authority over a member of the Armed Forces, or another person designated by such a commander to receive PHI to carry out an activity under that commander’s authority. Other appropriate authorities include any official designated for this purpose by the Secretary of Defense, the Secretary of the applicable Military Department, or the Secretary of Homeland Security (for Coast Guard activities not under the Navy).

FURTHER DISCLOSURES

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

ACCOUNTING OF DISCLOSURES

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



i PHIMT ASSISTANCE

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

MENTAL HEALTH AND/OR SUBSTANCE ABUSE DISCLOSURES

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

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

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

RECOMMENDED MILITARY TREATMENT FACILITY (MTF) POLICIES AND PROCEDURES

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

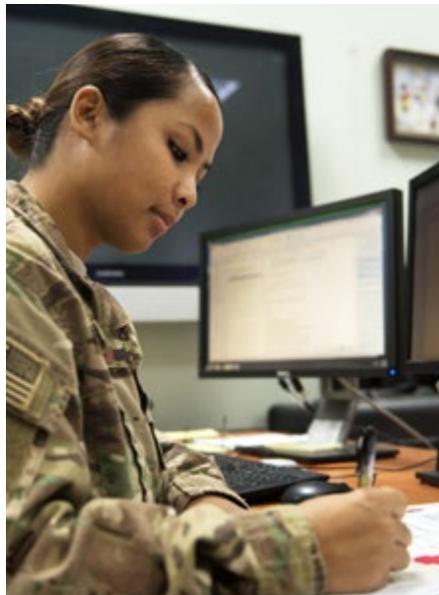
1. Designate specific MTF personnel with authority to release PHI to commanders
2. Maintain documentation of commanders/designees to whom Service members’ PHI may be disclosed
3. Train personnel on circumstances where PHI disclosures to military command authorities are appropriate
4. Educate personnel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



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

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

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



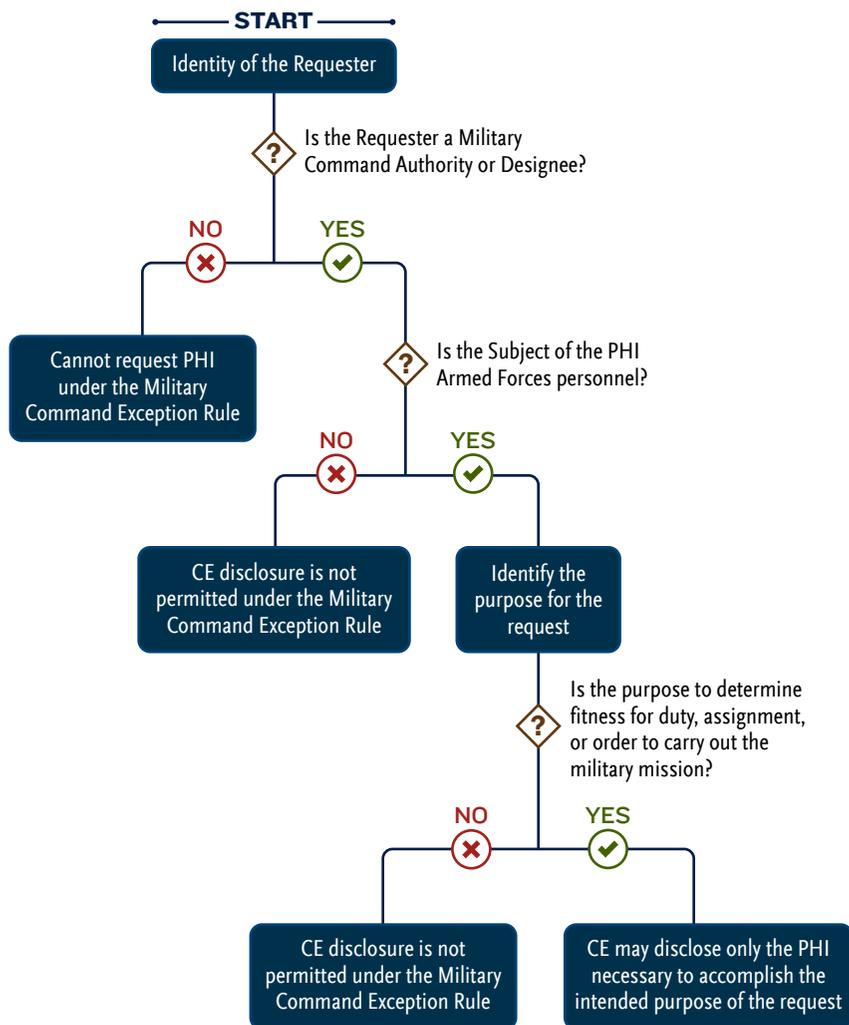
WHAT IS “NECESSARY TO ASSURE PROPER EXECUTION OF THE MILITARY MISSION?”

Under paragraph C7.11.1.3 of DoD 6025.18-R, 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 (DoDD) 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 DoDD 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



MILITARY COMMAND EXCEPTION DISCLOSURES



INTERCONNECTEDNESS

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

LOOKING AHEAD

Revisions to DoD 6025.18-R (currently in coordination) will add clarity to the military command exception and its applicability within the MHS, including:

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



**POINT OF CONTACT**

DHA.PrivacyMail@mail.mil for questions regarding the HIPAA Privacy Rule and the Military Command Exception

**RESOURCES****DoD Health Information Privacy Regulation and Instruction**

DoD 6025.18-R, January 24, 2003
(currently under revision),
DoDI 6025.18, December 2, 2009

DoD Privacy Program

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

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

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

HIPAA Privacy Web Page

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

DHA Privacy Military Command Exception Web Page

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

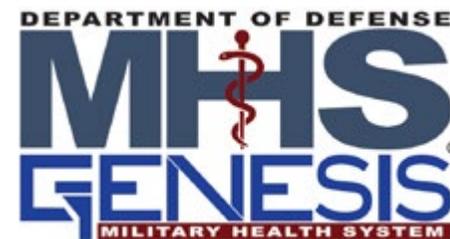


MHS GENESIS AND OTHER EMERGING TECHNOLOGIES

Riding the Wave: The MHS GENESIS Roll Out

Market dynamics and government action continue to transform the healthcare market. The Health Information Technology for Economic and Clinical Health Act provided incentives to increase the adoption of electronic health records (EHRs). EHRs have served as a major technology catalyst by providing the foundational data stores for massive amounts of information. Although the details have to be worked out, the Department of Veterans Affairs (VA) and DoD are now slated to be on the same EHR platform, a potentially synergistic development that will hasten the consolidation of disparate healthcare information systems and improve the efficiency and effectiveness of information sharing.

DoD continues to be a leader in applying emerging technologies to health care. With the first wave of the MHS GENESIS implementation over the last year, DoD has taken another bold step to respond to the transforming healthcare market. MHS GENESIS will eventually replace the Armed Forces Health Longitudinal Technology Application (AHLTA), Essentris®, and the Composite Health Care System (CHCS) by consolidating and managing data that was stored in the three systems.



Implementation of MHS GENESIS is occurring in a turbulent environment marked by changing regulations and a healthcare market that is rapidly transforming as a result of mobile technologies.

The continued implementation of MHS GENESIS will cause cascading changes. The MHS is consolidating the information technology infrastructure so there is one network, one data center, and one configuration and strategy to ensure all users and providers are on the same page. Doctors, nurses, and providers will see an updated system that standardizes core applications. Providers and patients will have reliable and secure access to medical information on their mobile devices. The mechanisms to share information both internally and externally will be affected as well.

THE IMPACT OF NEW SYSTEMS AND MOBILE TECHNOLOGIES

The rapid introduction of new technologies raises many significant privacy issues. Among the many areas under scrutiny is the privacy and security risk posture of new systems. Information systems must meet strict privacy and security requirements before they are given approval to start operating in the DoD environment. Before a new system can be deployed, it must undergo an authorization review process based on the DoD Risk Management Framework (RMF), culminating in the authority to operate (ATO). These requirements are referred to as controls. Security controls have been in place for a long time and while complicated, are well understood by individuals assigned to assess whether they have been satisfied.



Historically, the ATO process has focused on these security risks, but the RMF process has expanded its framework to include specific privacy risks. Therefore, a specific set of controls around privacy (collectively referred to as Appendix J controls) must now be applied; the DHA Privacy Office has been working energetically with other subject matter experts across DoD and the federal privacy community to implement these controls.

Mobile technologies pose unique threats to not only the security and privacy of information they maintain and transmit, but can also present real military challenges. These devices are often owned by the individual, not DoD, and are therefore harder to manage. The regulatory framework for mobile technologies is nascent and as they evolve, DoD must update its policies constantly to respond to the new capabilities they offer. Currently, the DHA Privacy Office provides input on specific Terms of Use and Privacy Policies. This information is typically published on the device so that individuals who access the technologies understand how their protected health information will be maintained, used, and possibly shared. While the information serves as a first line of defense, its effectiveness is unclear because mobile technology users often bypass the warnings and potential issues they address.

VIEWERS

DoD continues to consolidate its viewers into one because currently, DoD uses multiple mechanisms to view electronic data received from other organizations. The Joint Legacy Viewer (JLV) enables DoD and the VA to see health data from military treatment facilities and the Virtual Lifetime Electronic Record (VLER) viewer allows insight into health data generated by participants in the eHealth Exchange. Transitioning to one viewer will entail interim steps, such as the current consolidation of the JLV and VLER viewers into the Joint Legacy Viewer – Health Information Portal. The JLV is becoming the primary viewer used by the MHS.



INTERCONNECTEDNESS

The MHS supports the general privacy principle that individuals should have a right to participate in deciding how their data can be used and disclosed. As a result, the MHS allows non-active duty beneficiaries to opt out of sharing their information with other organizations. In summary, for the selected areas where the VLER capability is available, the health data for non-active duty beneficiaries is shared with external providers unless the beneficiary informs the MHS that he/she would like to opt out of information sharing. DHA has a process in place to identify, prioritize, and onboard private partners who may strengthen and improve information sharing and thus the quality of care provided to beneficiaries.



LOOKING AHEAD

MHS GENESIS has completed its first wave of the implementation process with Naval Hospital Bremerton, Madigan Army Medical Center, and Naval Hospital Oak Harbor following Fairchild Air Force Base's initial implementation which was on February 7, 2017. Additional work will be done to build interfaces and ensure that operations are streamlined to the greatest extent possible. Also, more capabilities will be added to the Initial Operating Capability, and lessons learned will be analyzed and resolved as the process continues to make the system more robust.



 **POINT OF CONTACT**

DHA.PrivacyMail@mail.mil for questions related to MHS GENESIS, Health Information Exchange, or other emerging technologies

 **RESOURCES**

MHS GENESIS Web Page
<https://www.milsuite.mil/book/groups/mhs-genesis>

Assistant Secretary of Defense for Health Affairs Memorandum
 Recommended Best Practices for Engaging with Health Information Exchange Organizations, April 5, 2012

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

DoD Health Information Privacy Regulation
 DoD 6025.18-R, DoD Health Information Privacy Regulation, January 24, 2003 (currently under revision)

HIPAA Privacy Rule
 45 Code of Federal Regulations (CFR) Parts 160 and 164

HIPAA Security Rule
 45 CFR Parts 160, 162, and 164

Security of Individually Identifiable Health Information in DoD Health Care Programs
 DoD Instruction 8580.02, August 12, 2015

DHA's CIVIL LIBERTIES PROGRAM

Safeguarding Civil Liberties

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

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

referred to as the DHA Privacy and Civil Liberties Office (Privacy Office). The DHA Privacy Office Chief has been designated by the DHA Director as the DHA CLO.

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

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

In Administrative Instruction (AI) 64, it is DHA policy to protect the privacy and civil liberties of DHA employees, Service members, family members, and the public with whom they come into contact to the greatest extent possible, consistent with operational requirements. When faced with questions concerning the potential impact that DHA employees' and contractors' work may have on an individual's civil liberties, please contact the DHA Privacy Office for guidance. The DHA Civil Liberties Program has won awards for its Outstanding Program in 2013, 2014, and 2015 and was designated the Top Program for 2014 and 2015 among DoD components. The model program evaluation process was discontinued by the Defense Privacy, Civil Liberties, and Transparency Division in 2016 because substantial progress was achieved by component civil liberties programs across DoD.

i CIVIL LIBERTIES TODAY

Carpenter v. United States. On November 29, 2017, the United States Supreme Court heard oral arguments on whether the Fourth Amendment was violated where the government accesses an individual's smartphone/cellphone location records without a warrant. The Court will publish its decision prior to the conclusion of the October 2017 Term, which ends in June 2018.

The decision is expected to clarify law enforcement agencies' ability to obtain smartphone/cellphone data collected by third-party communication providers in light of the Fourth Amendment. This case is considered one of the most important Fourth Amendment cases that the Supreme Court has heard in decades.



KEY TERMS

Chief CLO – 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 United States Code 2000ee-1) and the DoD Civil Liberties Program.

guaranteed by the Bill of Rights – the first 10 Amendments to the United States Constitution – such as freedom of speech, press, religion, and due process of law.

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

Civil Liberties – Offer protection to individuals from improper government action and arbitrary government interference. They are the freedoms

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

BILL OF RIGHTS	
The First Ten Amendments of the United States Constitution, also known as the Bill of Rights, offer the following civil liberties protections:	
First Amendment	Freedom of speech, religion, press, peaceful assembly, and the right to petition the government for a redress of grievances
Second Amendment	Right to bear arms
Third Amendment	Right not to have soldiers quartered in private residences without the consent of the owner
Fourth Amendment	Freedom against unreasonable searches and seizures
Fifth Amendment	Right against self-incrimination and to not be deprived of life, liberty, or property, without due process
Sixth Amendment	Right to a speedy trial
Seventh Amendment	Right to a trial by jury in cases over twenty dollars
Eighth Amendment	Freedom from cruel and unusual punishment
Ninth Amendment	Protects "non-enumerated rights" (e.g., right to travel, right to a presumption of innocence)
Tenth Amendment	The reservation of "States' Rights" – This Amendment makes it explicit that the Federal Government is limited only to the powers granted in the Constitution

INTERCONNECTEDNESS

Civil liberties sometimes intersect with Equal Employment Opportunity (EEO) and Human Resource (HR) matters as it relates to workforce complaints, which may involve alleged civil liberties violations and complex EEO and HR issues, as well.



LOOKING AHEAD

Privacy and United States Civil Liberties

Technological advances in areas such as surveillance, Internet and smartphone/cellphone/mobile, location tracking, medicine, and genetics continue to surpass existing privacy protections. In the wake of these innovations, privacy protections must evolve while continuing to focus on an individual's right to maintain control and security over their personal information as well as to ensure that civil liberties are strengthened, not diminished.

Privacy and (International) Civil Liberties

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



POINT OF CONTACT

DHA.Civil-Liberties@mail.mil
for DHA civil liberties-related questions

RESOURCES

Implementing Recommendations of the 9/11 Commission Act of 2007
Public Law 110-53

DoD Civil Liberties Program
DoD Instruction (DoDI) 1000.29, May 17, 2012

Organizational Placement and Structure of DoD CLO Functions
DoD Directive, December 14, 2009

Protection of Civil Liberties in the DoD
DoD, Office of the Secretary of Defense, 12888-10, November 1, 2010

DoD Health Information Privacy Regulation
DoD 6025.18-R, January 2003 (currently under revision)

Security of Individually Identifiable Health Information in DoD Health Care Programs
DoDI 8580.02, August 12, 2015

Civil Liberties Program Case Management System
Director of Administration and Management 01, January 19, 2011

DHA Civil Liberties Program
DHA AI, Number 64, June 14, 2017



FREEDOM OF INFORMATION ACT

Access to Records through the Freedom of Information Act (FOIA) or the Privacy Act of 1974

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 FOIA 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 FOIA requests or administrative appeals which are beyond the statutory time period for a response.

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



Consultation – The procedure whereby the agency responding to a FOIA request first forwards a record to another agency for review because the other agency has an interest in the document. Once the consulting agency finishes reviewing the record, it responds back to the forwarding agency. That agency, in turn, responds to the FOIA requester.

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

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

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

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

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

i 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

Partial Grant/Partial Denial

– An agency decision in response to a FOIA request to disclose portions of 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 FOIA request or administrative appeal for which an agency has not taken final action in all respects.

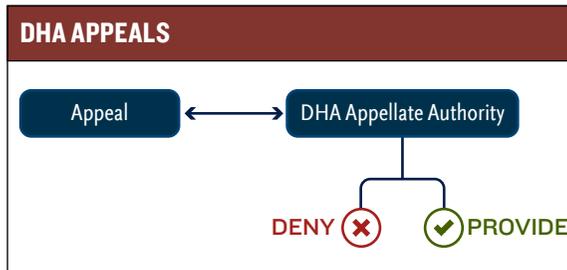
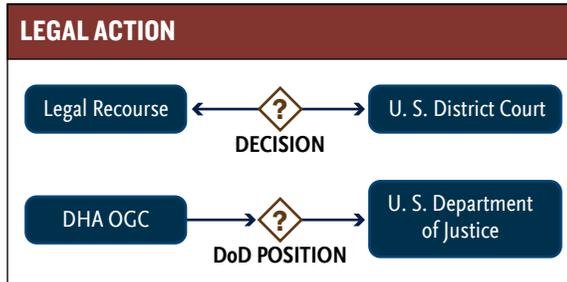
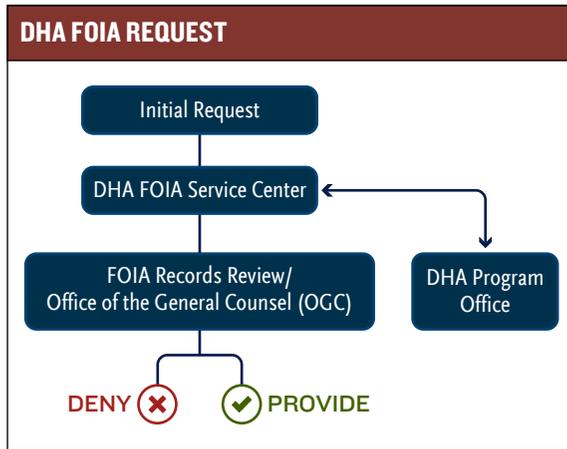
Perfected Request

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

Request Type

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

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



ACCESS UNDER THE PRIVACY ACT OF 1974

The Privacy Act allows individuals to:

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

DHA FOIA SERVICE CENTER

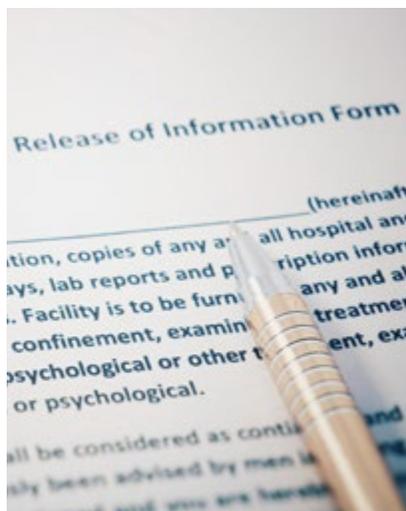
The DHA FOIA Service Center processes both FOIA requests and Privacy Act requests for the DHA. If a workforce member receives requests for information, please contact the DHA FOIA Service Center using the following information: 703-275-6363 or DHA.FOIA@mail.mil.

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



INTERCONNECTEDNESS

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



LOOKING AHEAD

Last year, the DHA FOIA Service Center began implementing the changes initiated by the FOIA Improvement Act of 2016. The Act amended key FOIA guidelines pertaining to fees, appeal timeframes, the FOIA Reading Room, and preemptive release activity. These requirements have impacted the DHA FOIA Service Center’s templates and standard operating procedures.

In addition, the Act created requirements for agencies to provide dispute resolution services via FOIA Public Liaisons and the United States National Archives and Records Administration Office of Government Information Services. In addition, the Act expanded the window for appealing a FOIA decision from 30 to 90 days. The Act also codifies the Department of Justice “foreseeable harm” and “proactive disclosures” standards by requiring agencies to “make available for public inspection in an electronic format,” records “that have been requested three or more times.” Overall, via the Act, Congress has worked to make FOIA more responsive, uniform, and digitized for the future.

Along with a proactive disclosure amendment, the Act promotes uniformity in FOIA processing by amending Section 3102 of the Federal Records Act, 44 United States Code § 3102, to include a requirement that agencies use to establish processes for identifying records of general public interest and for posting them in publicly accessible electronic format expeditiously. This final piece will require the DHA FOIA Service Center to keep the FOIA Reading Room updated more often and more thoroughly.

POINT OF CONTACT

DHA.FOIA@mail.mil for FOIA-related questions or for requester status updates

RESOURCES

Exemptions and/or the FOIA Process

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

FOIA Electronic Reading Room

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

Appeals or Complaints

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

Office of Management and Budget’s FOIA Web Page

<https://www.whitehouse.gov/omb/freedom-information-act-foia>

Executive Order 13489 – Presidential Records

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

OPEN Government Act of 2007

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

DoD Privacy Program

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



