

DHA Privacy and Civil Liberties Office

HEALTH INFORMATION  
PRIVACY AND SECURITY



# TRAINING MANUAL

MAY 2020



## **DHA PRIVACY AND CIVIL LIBERTIES OFFICE**

### **MAILING ADDRESS**

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

703-275-6363  
DHA.PrivacyMail@mail.mil

# DHA PRIVACY AND CIVIL LIBERTIES OFFICE

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

The mission of the DHA Privacy Office is to ensure vigilance in the protection of privacy information and to promote compliance across the DHA. The annual Health Information Privacy and Security (HIPS) training is one of the ways the DHA Privacy Office provides hands-on training to DHA personnel in support of our mission. Although we were not able to connect in person this year due to the COVID-19 pandemic, the DHA Privacy Office has prepared this training manual to serve as a reference for all privacy-related matters. This manual contains an overview of key programs, guidelines, initiatives, policy and procedure updates, resources, contact information, and tools that will help inform your privacy compliance efforts. The manual also includes information on how the DHA Privacy Office is addressing the transition of privacy compliance responsibilities as part of the 2017 National Defense Authorization Act.

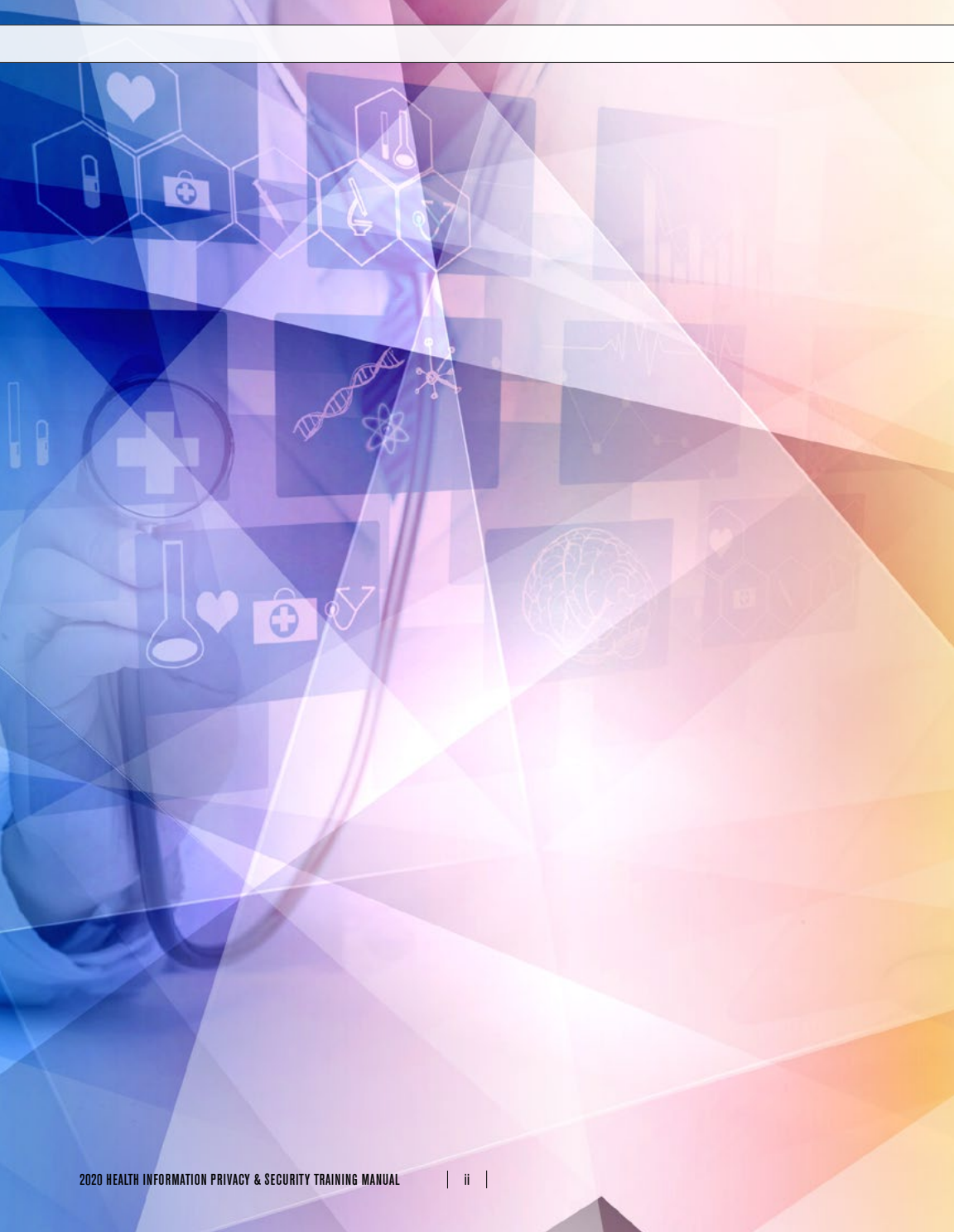
The manual may be accessed electronically on the DHA website at: <http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Act-and-HIPAA-Privacy-Training/Training-and-Awareness>.

Please do not hesitate to reach out to myself or my team with any questions about privacy compliance. Thank you for helping to protect the important information of which we are entrusted.

Sincerely,



Chief, DHA Privacy and Civil Liberties Office



# TABLE OF CONTENTS

|  |    |
|--|----|
| Introduction.....                                    | 2  |
| Federal Privacy Compliance .....                     | 5  |
| HIPAA Privacy.....                                   | 14 |
| HIPAA Security.....                                  | 23 |
| Privacy Risk Management .....                        | 30 |
| HIPAA Transactions, Code Sets, and Identifiers ..... | 34 |
| Data Sharing .....                                   | 38 |
| Breach Response.....                                 | 42 |
| Military Command Exception .....                     | 48 |
| MHS GENESIS and Other Emerging Technologies .....    | 54 |
| DHA’s Civil Liberties Program.....                   | 58 |
| Freedom of Information Act.....                      | 62 |



# 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. The 2017 National Defense Authorization Act (NDAA) was the catalyst for further collaboration across the MHS and the Services, impacting every division and directorate of DHA, including the DHA Privacy and Civil Liberties Office (Privacy Office).

In fulfilling its mission to ensure vigilance in the protection of privacy information and promote compliance across the DHA, the Privacy Office is guided by the four priorities for the DHA:

1. Great Outcomes
2. Ready Medical Force
3. Satisfied Patients
4. Fulfilled Staff

These priorities inform how each law, regulation, and policy is implemented by the DHA Privacy Office and also provide the foundation for the changes required by the NDAA. The DHA Privacy Office will continue to work with the Services to strengthen the safeguards for our beneficiaries' data and provide the framework for them to confidently share the information our providers need to deliver comprehensive medical care.







## DHA PRIVACY OFFICE

The DHA Privacy Office, which falls under DHA J-1, the Administration and Management Directorate, oversees the protection of personally identifiable information and protected health information within the MHS. The MHS is one of the largest integrated healthcare delivery systems in the United States, serving over 9.5 million eligible beneficiaries 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 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
- Upholding Civil Liberties

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



# FEDERAL PRIVACY COMPLIANCE

## Privacy Requirements

All federal executive branch agencies, whether a HIPAA covered entity or not, must comply with general federal privacy laws and regulations. These requirements are found in the Privacy Act of 1974 (Privacy Act), the E-Government Act of 2002, and other associated regulations and guidance. DoD implements the Privacy Act through the DoD Privacy Program Publication.

### THE PRIVACY ACT

The Privacy Act establishes safeguards and protects the personally identifiable information (PII) of citizens and permanent residents when that information is stored in a government system of records (SOR) and retrieved by a personal identifier (such as a name, ID number, etc.). The Privacy Act mandates that the United States Government collect only the PII needed to conduct government business and ensure that information is accurate, relevant, timely, and complete. The Privacy Act imposes civil and criminal penalties for noncompliance. It was designed in part to embody the Fair Information Practice Principles established in 1973 by the Department of Health, Education, and Welfare (predecessor to the Department of Health and Human Services (HHS)). These principles 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 maintained in a Privacy Act SOR upon written request. The individual may also seek amendment of the information held about them if they can demonstrate it is inaccurate. 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** – Whenever a contractor manages or operates a SOR on behalf of a federal agency, the Privacy Act requirements apply to that contractor as though it were a federal agency. Consequently, oversight and monitoring of contractors' work by government sponsors is essential for an agency's compliance.

**Matching Agreements** – When agencies 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 may 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.

*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

**THE FAIR INFORMATION PRACTICE PRINCIPLES**

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.

|                                 |   |
|---------------------------------|---|
| <b>Minimization</b>             | Agencies should limit the collection of PII to only that which is relevant and necessary to accomplish the mission, obtained by lawful and fair means, and with the knowledge or consent of the data subject  |
| <b>Quality and Integrity</b>    | To the extent feasible, agencies must ensure that collected data is relevant to the purposes for which it is to be used and is relevant, accurate, timely, and complete   |
| <b>Purpose Specification</b>    | Agencies must determine the specific purpose or purposes for which information on individuals is to be collected and used at the point of initial data collection   |
| <b>Use Limitation</b>           | 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   |
| <b>Security</b>                 | Agencies must protect the confidentiality, integrity, and availability of the data using appropriate administrative, technical, and physical safeguards   |
| <b>Transparency</b>             | Agencies must provide notice of systems collecting PII, and information about those systems including purposes and uses   |
| <b>Access and Amendment</b>     | Individuals should be provided access to their own information within a SOR, and should be able to correct inaccurate data  |
| <b>Accountability</b>           | 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  |
| <b>Individual Participation</b> | Agencies should involve the individual in the overall process of using PII, including seeking consent for creation, collection, use, disclosure, and processing of PII. Procedures should be established to provide individuals with the ability to file privacy-related complaints and inquiries |

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 – fostering agency accountability through public notice.

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



## 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 records, 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 in response 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 breach response.

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

## KEY E-GOVERNMENT ACT AND FISMA REQUIREMENTS

According to the E-Government Act and FISMA of 2002, as well as DoD Instruction (DoDI) 5400.16, **Privacy Impact Assessments (PIAs) are required for all Federal information systems that collect, maintain, and disseminate PII.** Federal information systems containing PII require a PIA that must be renewed every three years, or when a significant change occurs to the system. 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, in order to ensure IT complies with all pertinent requirements and adequately addresses any risk to privacy.



### 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 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.” In addition, the revised OMB Circular A-130, *Managing Information as a Strategic Resource* (released July 16, 2016), ties 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 the information 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
- Other 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. For further information on available trainings, contact the DHA Privacy Office.

**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.



**AWARENESS**

If PII is collected, a PIA is required for:

- Existing DoD information systems and electronic collections for which a PIA has not previously been completed, including systems that collect PII about DoD personnel and contractors
- New IT, or electronic collections, or
- DoD IT or electronic collections with a completed PIA, when change creates new privacy risks

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

**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?  |
| 2 | If the answer to question 1 is yes, does the information collected include PII?  |
| 3 | <p>If the answer to question 2 is yes, is the information retrieved by the individual's unique identifier?</p> <p>✗ Answer no if the system can retrieve by a unique identifier, but does not</p> <p>✗ Answer no if the system only retrieves by non-unique identifiers, such as a case number</p> <p>✗ Answer no if the system only retrieves by a unique identifier when an individual asks for his or her own records</p> |

Note that the form of the information (paper, electronic, or a combination thereof) is irrelevant. 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>).





## PLANS FOR TRANSITION

Since the implementation of the National Defense Authorization Act of 2017, the scope of information systems currently being assessed for privacy compliance has broadened. Currently, the DHA Privacy Office is working to assess the PIA status of all information systems on the MHS Medical Community of Interest (Med-COI) listed in the Enterprise Mission Assurance Support Service (eMASS), as well as the DoD Information Technology Portfolio Repository. Based on an analysis of the information systems in eMASS, the Federal Privacy Compliance (FPC) team and DHA Cybersecurity division formed a workgroup to improve the privacy and security compliance posture of DHA. The FPC team also works closely with Service points of contact (POC) to facilitate the transition of information systems that the Services have already determined will transition to the DHA. The FPC team also attends the weekly CIO workgroup meetings and provides updates once a month. The FPC team hosts a monthly FPC sub-workgroup meeting to inform the Services of updates regarding transitions for Federal privacy as well as obtain information from the Service POC regarding their expectations and requirements.

Furthermore, if an information system transitions to the DHA, and the information system does not have a PIA, the system owner or program office is required to complete a Directives Division (DD) Form 2930, Privacy Impact Assessment (PIA). The DD Form 2930 is to be used for all information systems. An analysis of similar information systems used by each Service will be conducted to determine if the systems can be combined into one SORN. If so, the FPC team will guide the system owner or program office through the SORN writing process. The Services are not rescinding any SORNs currently, however when the Services determine to rescind or modify their SORNs, the FPC team will work closely with the Services. Lastly, the FPC team is working in conjunction with the DHA Forms Manager to transition Service forms to the DHA and the Information Management Control Officer to review surveys.

This transition has increased data challenges in the MHS to both the management of internal DHA enterprise data and the management of external data or stand-alone systems purchased at the component level. The FPC team is here to ensure that the information systems are privacy compliant; therefore, the team is here to assist the system owners/program offices.





## POINTS OF CONTACT

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

**DHA.PIA@mail.mil** for PIA/E-Gov related questions



## RESOURCES

**The Privacy Act of 1974**

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

**DoD Privacy Program**

DoD 5400.11-R, May 14, 2007

DoDI 5400.11, January 29, 2019

**DoD Privacy Impact Assessment Guidance**

DoDI 5400.16, revised August 11, 2017

**DHA Privacy and Civil Liberties Office Privacy Program Plan**

Revised on March 31, 2020

# 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 Instruction (DoDI) 6025.18, *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs*, and DoD Manual (DoDM) 6025.18, *Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs*; these Issuances replaced DoD 6025.18-R, the *DoD Health Information Privacy Regulation*, in March 2019. The DHA Privacy Office developed a crosswalk between DoD 6025.18-R and DoDM 6025.18 to help familiarize stakeholders with the updated content and organization.

### KEY TERMS

**Business Associate (BA)** – With respect to a DoD CE, a party that creates, receives, maintains, or transmits PHI on behalf of the DoD CE for a HIPAA-covered function or activity; or a party that provides legal, actuarial, accounting, consulting, data aggregation, management,

administrative, accreditation, or financial services to or for such DoD CE, where the provision of the service involves disclosure of PHI to that party. A DoD or other CE may be a BA performing HIPAA-covered functions on behalf of another DoD CE. Reference DoDM 6025.18, Paragraph 3.3.c.

### **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 DoDM 6025.18, Paragraph 3.3.c. 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, or a healthcare provider who transmits any health information in electronic form in connection with a standard transaction under Part 162 of Title 45, Code of Federal Regulations (CFR). CEs within DoD are generally defined or identified in DoDM 6025.18, Paragraph 1.1.a.(1)(a).

**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. Reference DoDM 6025.18, Paragraph 5.1.



**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 participate in certain joint activities. The MHS and certain elements of the United States Coast Guard are a single OHCA, under DoDM 6025.18, Paragraph 3.3.b. 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 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. Since 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. CE's workforce members must follow established policies and procedures when seeking to exercise their individual rights. Reference DoDM 6025.18, Paragraph 3.1.d.(6). When it comes to applying these rights in connection with a minor, the MHS applies the State law where the treatment is provided. Reference DoDM 6025.18, Paragraphs 3.2.b.(2)(a) and 4.5.g.(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. Reference DoDM 6025.18, Paragraph 5.1.

### 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. DoDM 6025.18, Paragraph 5.2.a., 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. DoDM 6025.18, Paragraph 5.2.b., 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). Reference DoDM 6025.18, Paragraph 5.3. Audit logs or access reports, which provide information on who has accessed PHI, are not part of a designated record set. Reference DoDM 6025.18, Paragraph 5.3.b.(1). 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 and 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. DoDM 6025.18, Paragraph 5.4, 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. DoDM 6025.18, Paragraph 5.5, 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. Reference DoDM 6025.18, Paragraph 7.2.a.

### MHS NoPP

The current MHS NoPP was issued by the DHA Privacy Office on October 1, 2013. 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 reference: <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. DoDM 6025.18, Paragraph 4.5.g., sets forth how DoD CEs determine who is the personal representative of an unemancipated minor, an adult, and an emancipated minor under applicable law.



### DHA HIPAA PRIVACY RULE WEB ASSESSMENT TOOL

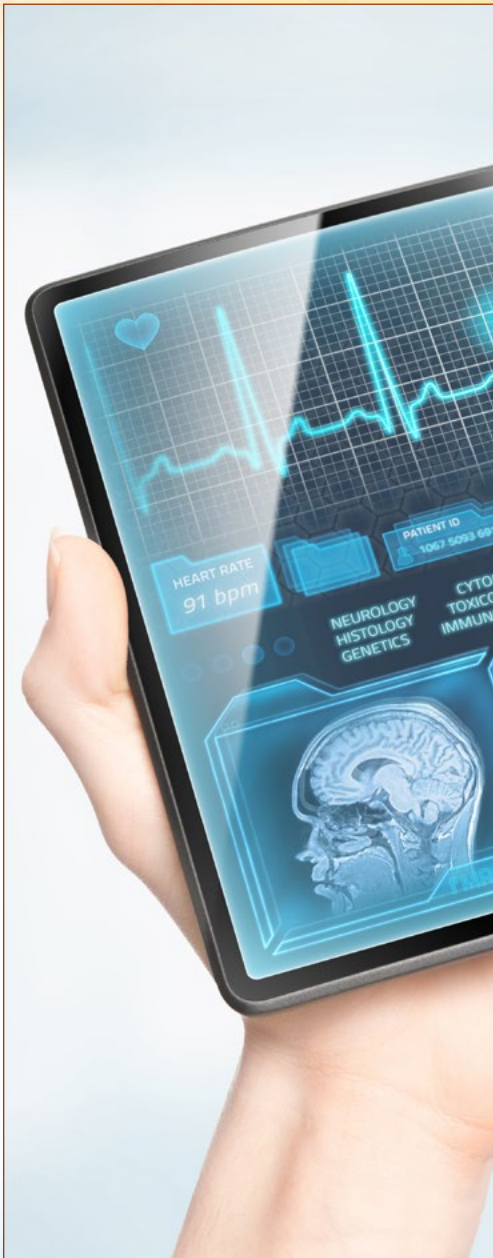
The DHA HIPAA Privacy Rule Web Assessment Tool is a comprehensive web-based instrument used to aid MTFs in assessing their compliance with the HIPAA Privacy Rule. Upon responding to a series of questions, the user will receive a customized assessment report identifying opportunities to enhance or develop 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.




### PLANS FOR TRANSITION

The DHA Privacy Office will serve as a source of guidance regarding the interpretation and implementation of the HIPAA Privacy Rule within the MHS and will continue to develop resources that are responsive to the needs of our stakeholders.


The DHA is responsible for the privacy protections to safeguard PHI and adhere to the DoD regulations and applicable federal privacy laws. To assist in ensuring compliance, the DHA Privacy Office has developed the Compliance Risk Assessment initiative to determine the Agency's privacy risk, overall compliance and to support the maintenance of a strong privacy compliance posture within the DHA. The results will assist DHA in continuing its efforts to develop, implement, and maintain policies and procedures that provide privacy protections for all PHI maintained by MTFs consistent with the HIPAA Privacy Rule. While MTF operations will be guided by overarching policies and procedural guidance issued by the DHA, the MTFs must also have in place local policies and procedures addressing the implementation of DHA policy. Such local policies and procedures are to be developed by the local HIPAA Privacy Officer, and then reviewed and approved by the DHA Privacy Office prior to implementation to ensure compliance with the requirements of the HIPAA Privacy Rule; this review will allow for the standardization of HIPAA compliance throughout the MHS enterprise.



 **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>

**Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs**  
DoDI 6025.18, March 13, 2019

**Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs**  
DoDM 6025.18, March 13, 2019

**HIPAA Privacy Rule**  
45 CFR Parts 160 and 164

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

**Crosswalk of DoD 6025.18-R and DoDM 6025.18**  
Accessible via: <https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS>

# 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)<sup>1</sup> when it is stored, maintained, and/or transmitted. Complying with HIPAA Security Rule business practices and information technology safeguards help medical facilities endure threats and hazards to ePHI daily.

### 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 (MTFs) (medical/dental)   |
| Individual and group health plans   | TRICARE Health Plan   |
| Healthcare clearinghouses   | Companies that perform electronic billing on behalf of MTFs   |
| Business associates (BAs)   | Healthcare services support contractors and other contractors that provide services that require access to protected health information (PHI) |

### RISK MANAGEMENT AND THE HIPAA SECURITY RULE

The HIPAA Security Rule requires CE and BA 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 BA to understand their technical capabilities, internal and external sources of ePHI, and known or potential threats and vulnerabilities in their environments.

<sup>1</sup> 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.

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.<sup>2</sup>

As organizations conduct HIPAA risk assessments, they may find that more stringent controls are appropriate than those which 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 for a legal opinion if they are considering tailoring or otherwise altering the security and privacy controls identified within the Privacy Overlays.

## **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 DoD 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 for 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* and SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.



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

## THE HIPAA SECURITY RULE SAFEGUARDS

**Administrative safeguards** are designed to protect ePHI ensuring confidentiality of information and to manage the conduct of the DoD CE's workforce using ePHI in their job performance. 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 DoDI 6025.18, *Health Insurance*

*Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs*, and DoD Manual (DoDM) 6025.18, *Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs*.

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



## 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 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. Based on DHA Administrative Instruction 81, *Employee Use of Information Technology (IT)*, September 15, 2015, MHS personnel shall not transmit sensitive information or PHI via the Internet/e-mail or other electronic means unless appropriate security controls (e.g., encryption, Public Key Infrastructure) are in place.



### STOP AND THINK – 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 government business
- ✓ Double check e-mail addresses before sending
- ✓ Only use authorized networks
- ✓ Always encrypt e-mails that contain personally identifiable information (PII) and PHI



## PLANS FOR TRANSITION

### DHA Privacy Office Compliance Risk Assessment (CRA)

The DHA is entrusted with a significant amount of PII and PHI. As part of our collective responsibility to safeguard this data, we must document our compliance with the applicable federal privacy laws and DoD implementing issuances including, but not limited to, the Privacy Act of 1974 and HIPAA. The DHA Privacy Office has developed the CRA Initiative to support the maintenance of a strong compliance posture within the DHA. The goals of the CRA are:

1. Provide a comprehensive assessment, with metrics, of the overall privacy and security-related compliance posture of all DHA assets
2. Assist all HIPAA Privacy and Security Officers across the enterprise in determining the risk and overall compliance for their respective organization(s)
3. Provide MTFs and Markets with a comprehensive risk assessment tool to assist in the assessment of the overall privacy and security compliance for their respective organization(s)
4. Maintain oversight of required regulatory compliance standards policies and procedures
5. Establish and recognize compliance best practices relative to the management of PHI and PII





## PLANS FOR TRANSITION (CONTINUED)

### DHA Privacy Office CRA (continued)

Since the National Defense Authorization Act of 2017 organized the MTFs under the administrative control of the DHA, the DHA Privacy Office has expanded both the scope and the reach of the CRA. This includes the Markets and MTFs under DHA's authority, direction, and control, which is in addition to the DHA Program Offices. Each MTF and/or Market, as appropriate will be asked to participate in the initiative. Participation requires the completion of a web-based questionnaire and a structured interview with individuals familiar with the office's work, privacy and security protections. The resulting information assists the DHA Privacy Office and DHA Leadership in assessing the compliance posture of DHA. All reviews are documented and a report highlighting findings and recommendations is provided to the participating offices and points of contact. Additionally, the CRA allows the DHA Privacy Office to provide education and outreach, enables offices to ask questions and obtain advice, and offers an opportunity for ongoing assistance and support to all levels of DHA staff.

The CRA questionnaire is hosted on the DHA LaunchPad website and is comprised of a full series of privacy questions and topics including the Privacy Act, Freedom of Information Act, HIPAA Privacy, HIPAA Security, Privacy Impact Assessments, Breaches, Civil Liberties, Privacy Training, and other general privacy topics. Some topics may only have a few questions, while others go much deeper. For example, the HIPAA Security section includes questions on every safeguard found within the HIPAA Security Rule. Those completing the questionnaire are not required to answer all the questions in one session but are able to save and continue at their convenience. Once all the questions have been completed, users must submit their answers. The DHA Privacy Office then reviews the responses and provides the specific follow-up as needed.

HIPAA Security Rule implementation and compliance is a major focus of the CRA. There are questions related to every administrative, physical, and technical safeguard found within the Security Rule, as well as the corresponding references to each regulation(s). Answering these questions will assist MTF HIPAA Security Officers to better understand the HIPAA Security compliance within the MTF as well as identify any areas of weakness. These questions can help form the foundation of a HIPAA Security Risk Analysis that is required by the HIPAA Security Rule.





### 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

**Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs**  
DoDI 6025.18, March 13, 2019

**Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs**  
DoDM 6025.18, March 13, 2019

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

**Security Controls for Federal Information Systems and Organizations**  
NIST SP 800-53, Revision 4, January 2015

# PRIVACY 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 and specific guidance for electronic protected health information (ePHI) on its transition through the Committee on National Security Systems Privacy Overlays Working Group. This group is one of several government working groups that develop tools to embed 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.

### **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 (GNSSI) 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 Personally Identifiable Information (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).<sup>1</sup>

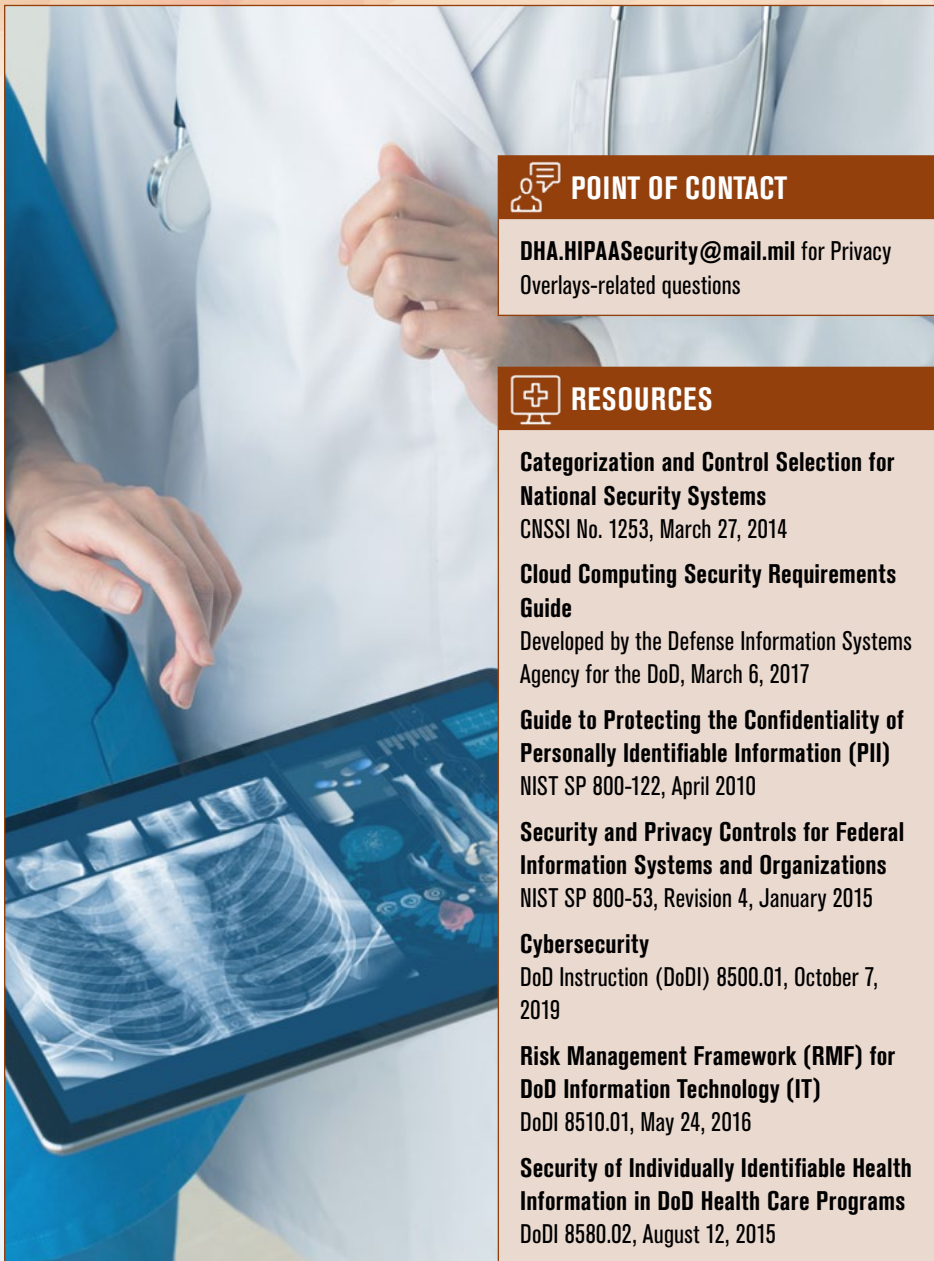
By definition, PHI is PII; thus, the laws, regulations, and other standards for safeguarding PII also apply to PHI. Therefore, the organization must follow the guidance contained in the Privacy Overlays to determine the PII confidentiality impact level of the information it owns or manages and apply 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.



### PLANS FOR TRANSITION

The soon to be released NIST SP 800-53, Revision 5 (Rev 5) publication is now fully integrating privacy controls into the security control catalog creating a consolidated and unified set of controls; while separating the control catalog from the control baselines. The security and privacy control baselines are projected for publication in 2020 as NIST SP 800-53B, *Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations*. Once Rev 5 is released, the DHA Privacy Office will work on revamping our processes and implementation for privacy compliance.

<sup>1</sup> 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.



### 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

**Cloud Computing Security Requirements  
Guide**

Developed by the Defense Information Systems  
Agency for the DoD, March 6, 2017

**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, October 7,  
2019

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

DoDI 8510.01, May 24, 2016

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

DoDI 8580.02, August 12, 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 Capability Portfolio Management (B-CPM) Office specifically 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.

HIPAA-mandated identifiers have included the Employer Identifier, the National Provider Identifier (NPI), and the Health Plan Identifier (rescinded by a Final Rule as of December 27, 2019). 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 and Procedure Coding System) are code sets required by HIPAA. HIPAA-mandated code sets may also be used for non-HIPAA purposes.



For implementation and compliance of mandated HIPAA TCS&I, the DHA's B-CPM Office's HIPAA TCS&I Program serves as the liaison and facilitator between the functional business process user communities (e.g., DHA/ Deputy Assistance Director (DAD) Financial Operations/Uniform Business Office) and technical system Program Offices (e.g. DHA/DAD for Information Operations/Solution Delivery Division). It also serves as the HIPAA TCS&I liaison and facilitator 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 Health Plan 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 provider identifiers such as the NPI in HIPAA transactions, etc.
- Collaboration with other Federal agencies, healthcare industry organizations, and other DHA offices
- Defense Medical Logistics as related to implementation and use of Unique Device Identifiers (UDI) for implantable medical devices, as components of UDI may be used in HIPAA transactions

### **i** 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. The following CEs need to comply:

- Providers (e.g., military treatment facilities (MTFs), 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., ePremis®, Emdeon®)
- Business associates of CEs (e.g., Defense Manpower Data Center/Defense Enrollment Eligibility Reporting System (DMDC/ DEERS), TRICARE Purchased Care Contractors)







## DID YOU KNOW DHA CONTRIBUTES TO HIPAA STANDARDS DEVELOPMENT?

DHA is a contributing member in the United States healthcare industry's collaborative process of developing and advancing HIPAA administrative electronic transaction standards. As a result, DHA helps to shape the future of meeting United States healthcare business requirements in HIPAA transactions that include Benefit Eligibility, Enrollment, Referrals, Claims, and Claim Payment. If you want to know more, please visit: <https://health.mil/About-MHS/OASDHA/Defense-Health-Agency/Resources-and-Management/HIPAA-Transactions-Code-Sets-and-Identifiers-Office>



## PLANS FOR TRANSITION

HIPAA TCS&I compliance activities will see minor changes as a result of DHA transition under the National Defense Authorization Act of 2017 Section 702. MTF systems that support HIPAA transaction standards for referrals and billing are already, and will continue to be, MHS enterprise-wide DHA centrally-managed systems. Primary interactions between the B-CPM HIPAA TCS&I Program and DHA functional business process offices will continue to be at the DHA headquarters level. One area of change may include implementations of newly named and adopted HIPAA TCS&I standards (by Final Rule in the Federal Register). There will be different paths of communications based on changes to, and new offices in, the MHS organizational and management structure (e.g., what had been interactions with the Services to facilitate communications to and from MTFs, are expected rather to be done within DHA communication channels).





### POINT OF CONTACT

**Dha.ncr.bus-info-mgt.mbx.hipaacs@mail@  
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/>

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

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

# DATA SHARING

## Requesting DHA Data

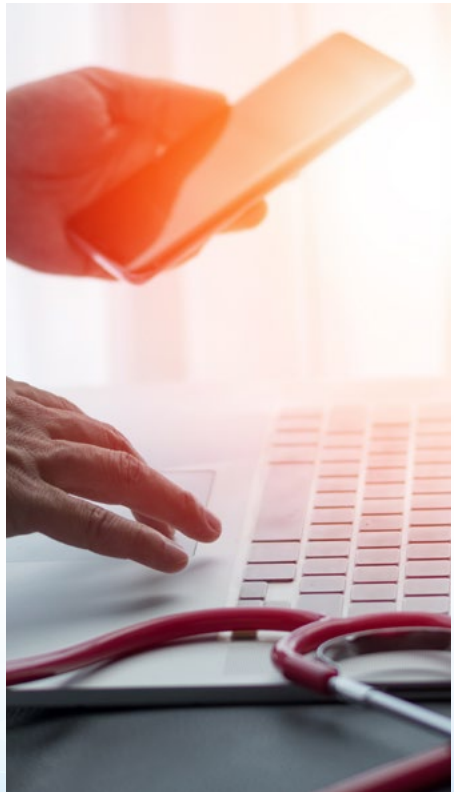
The DHA Privacy Office receives various types of data sharing requests for DHA data. Under its Data Sharing Program, the DHA Privacy Office reviews each request for compliance with applicable privacy and security regulatory requirements.

The DHA Privacy Office neither grants system access nor provides data extractions; however, prior to gaining access or 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.

### DATA SHARING PROGRAM

The Data Sharing Program was established within the DHA Privacy Office to:

- Confirm whether a requested use or disclosure of DHA data is permitted 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 ensure the requested data will be appropriately safeguarded. 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 received appropriate compliance reviews by an Institutional Review Board (IRB) or the DHA Human Research Protection Program and, if necessary, a separate HIPAA Privacy Board

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



### 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
- For non-government academic researchers, must have a grant, cooperative research and development agreement, or a binding agreement with a sponsoring government entity

**Government Sponsor** – The point of contact from within the sponsoring organization who assumes overall responsibility, on behalf of the government, for the expected use and protection of the data. This role may be filled by a civilian within DoD or an active duty Service member.



## ARE YOU READY TO SUBMIT A DSAA?

- ✓ Do you have all applicable pre-approvals required for this data use and disclosure?
- ✓ Have you completed the DSAA Pre-Requisites Checklist?
- ✓ Did you complete a DSAA?
- ✓ Have you provided a clear purpose for the data requested?
- ✓ Have you adequately described the process to receive, use, de-identify, store, publish, and/or report the data?
- ✓ Did both the Applicant and Government Sponsor initial the request?
- ✓ You can now submit the DSAA.

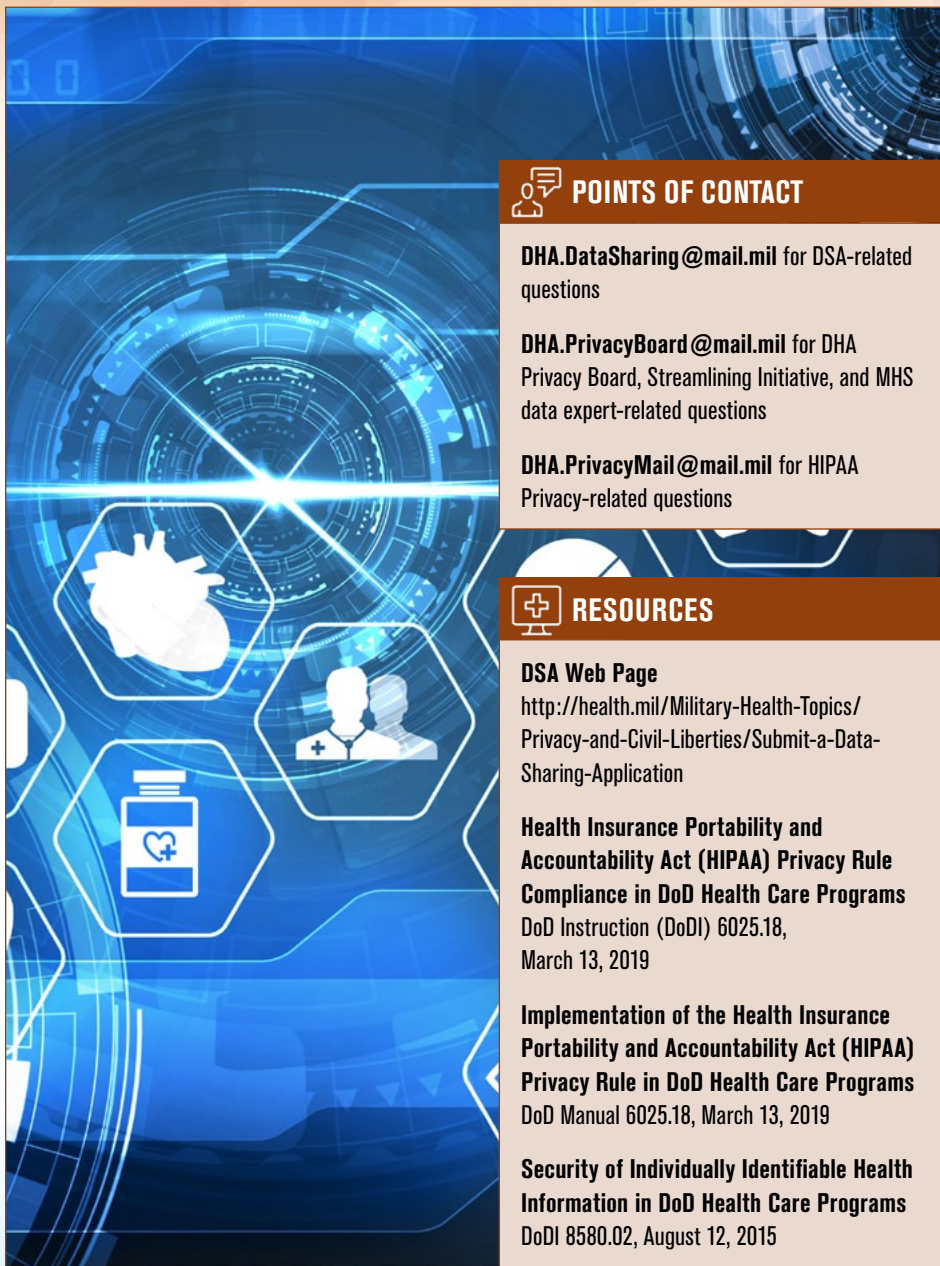


## PLANS FOR TRANSITION

**Streamlining the entire Data Sharing Program review process:** This streamlining consists of collaborating with data managers/stewards to assist with data requests, creating a pre-requisite checklist to assist data requestors before submitting the DSAA, and redesigning the DSAA to be more user-friendly.

**Restructuring research HIPAA Privacy Rule review:** In continuation of the DHA Privacy Office efforts to streamline 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, the DHA Privacy Office delegated HIPAA Privacy Rule reviews to IRBs so that IRBs can simultaneously conduct both reviews. Before conducting these reviews, IRBs will have to meet a list of requirements, including, but not limited to, taking Joint Knowledge Online training, “DHA-US096: HIPAA Privacy Rule Compliance Training for Institutional Review Boards and HIPAA Privacy Boards” and requiring researchers to use standardized templates available on electronic IRB and provided by the DHA Privacy Office. Researchers will submit the IRB HIPAA Privacy Rule findings along with the DSAA.

With the transition of military treatment facilities into the DHA, the DHA Privacy Office anticipates a significant increase in the number of information systems managed by DHA, resulting in an increase in the number of DSAs the DHA Privacy Office will receive for the use of the additional data. The restructuring will facilitate efficient review of the DSAs while maintaining adherence to privacy compliance requirements.



## 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>

**Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs**  
DoD Instruction (DoDI) 6025.18,  
March 13, 2019

**Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs**  
DoD Manual 6025.18, March 13, 2019

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

# 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 breach compliance. Mishandled or misused personally identifiable information (PII) or protected health information (PHI) may result in a breach or HIPAA Privacy violation. This chapter is designed to serve as a quick reference on how to prevent and mitigate breaches.

### 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.

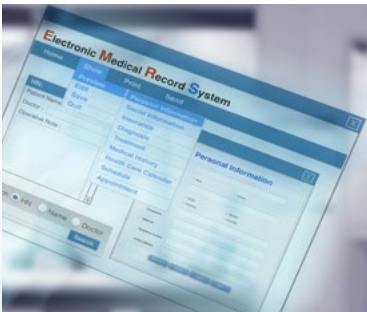
### BREACH REPORTING

Upon discovery of an actual or possible breach, reporting must take place in accordance with the local incident response protocol. Please see the next page for reporting protocol procedures.

*NOTE: These also apply to military treatment facilities (MTFs) transitioning to DHA in accordance with the Fiscal Year (FY) 2017 National Defense Authorization Act (NDAA).*



|  |
|--|
| <b>FOR DHA MTFs, COMPONENTS,<br/>AND PURCHASED CARE<br/>CONTRACTORS</b>  |
| <b>LEADERSHIP:</b> <ul style="list-style-type: none"> <li>• Immediately</li> </ul>   |
| <b>NATIONAL CYBERSECURITY AND<br/>COMMUNICATIONS INTEGRATION<br/>CENTER:</b> <ul style="list-style-type: none"> <li>• Within one hour of a confirmed cyber security incident</li> </ul>  |
| <b>DHA PRIVACY AND CIVIL LIBERTIES<br/>OFFICE:</b> <ul style="list-style-type: none"> <li>• Within one hour of discovery (for DHA MTFs and Components)</li> <li>• Within 24 hours of discovery (for Purchased Care Contractors)</li> </ul> |
| <b>DEFENSE PRIVACY, CIVIL LIBERTIES,<br/>AND TRANSPARENCY DIVISION:</b> <ul style="list-style-type: none"> <li>• Within 48 hours</li> </ul>  |
| <b>HHS:</b> <ul style="list-style-type: none"> <li>• Within 60 days of discovery if 500 or more individuals are impacted</li> <li>• Within 60 days of the close of the calendar year if less than 500 individuals are impacted</li> </ul>  |



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
- Make sure to log out of all systems containing sensitive information before leaving workstations
- 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
- Administer recurring HIPAA and Privacy Act training and refresher/remedial training, when necessary
- Ensure reminder banners appear upon access of systems containing PII/PHI
- Include breach awareness posters in break rooms and other high traffic areas



# 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

- Inform 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 prevent further disclosure such as retrieving or destroying documents

## 4. MITIGATION

Communicate with potentially affected individuals, investigators, and other involved entities.

Additional actions may include:

- Coordinate with business partners to issue a press release for large-scale breaches
- Offer credit monitoring services to individuals whose information was compromised
- Apply administrative, physical, and technical safeguards
- Ensure the proper retrieval, deletion, or destruction of improperly disclosed PHI/PII

## 5. ERADICATION

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

- Quarantine infected files and systems and deploy application patches
- Update beneficiary contact information

### 6. RECOVERY

Restore business operations to normal status

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

### 7. FOLLOW-UP

Take necessary actions to prevent future occurrences

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

## 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 initial and recurring 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 consistent 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

The Incident Response Team (IRT) and Breach Response Requirements re-signed on September 15, 2015, AI 71 outlines the processes and procedures for assessing and responding to confirmed or suspected breaches occurring within DHA. All workforce members must follow these guidelines when an actual 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 is planned for September 10, 2020, at the Defense Health Headquarters.

*NOTE: All assigned or attached Service members, federal civilians, contractors, and other personnel assigned temporary or permanent duties at DHA are subject to the breach response requirements included in DHA AI 71. The DHA Privacy Procedural Instruction (PI), with input from the Services, will be published in the near future, standardizing breach reporting responsibilities across the enterprise.*

## 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 staff members are trained appropriately

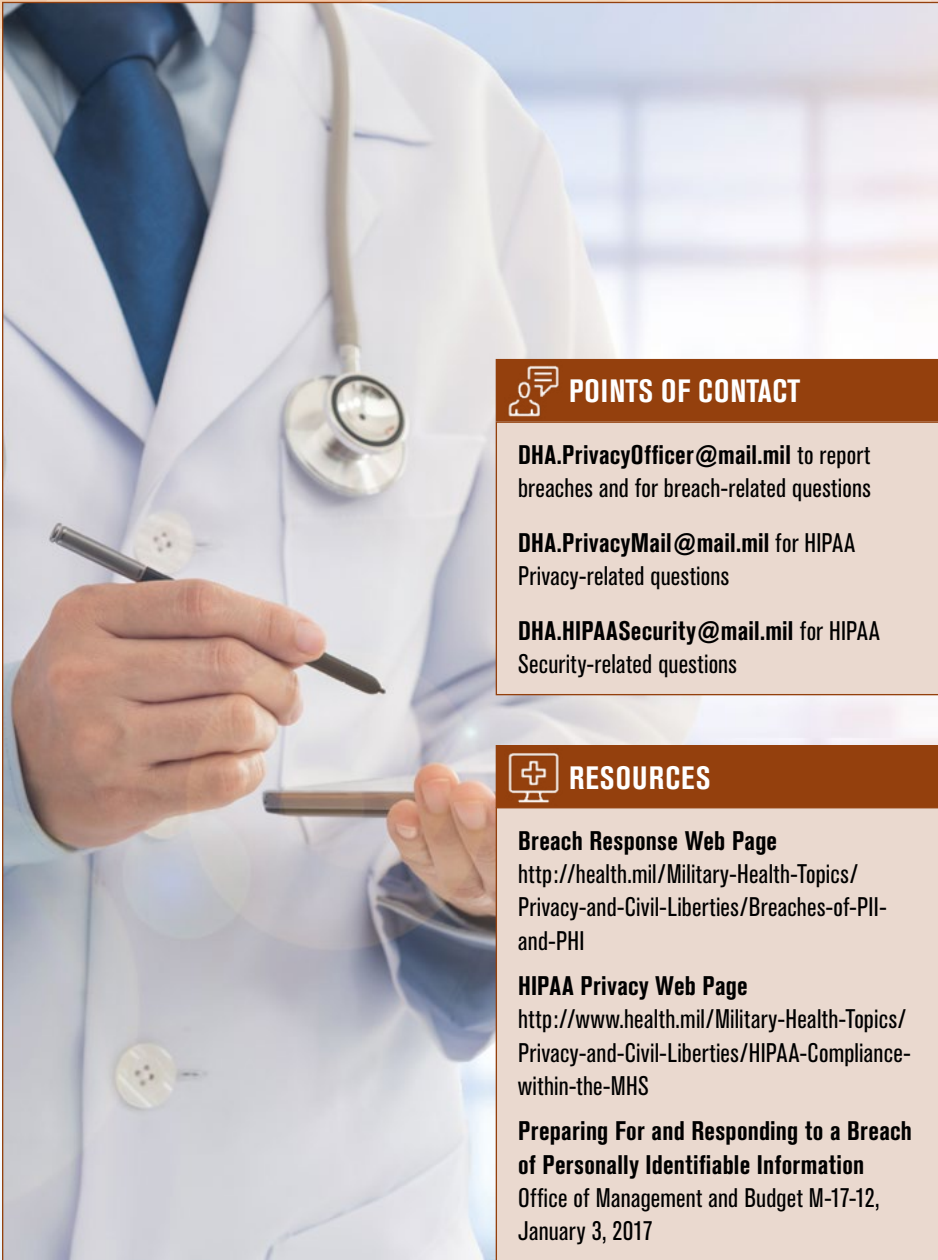


## PLANS FOR TRANSITION

In its future state, the DHA Privacy Office will support the enterprise to include the DHA Markets, MTFs and headquarters by serving as the single source for breach reporting.

All DHA Markets and MTF workforce members are required to complete the DD Form 2959 Breach Notification Form for any potential or actual breach of PHI/PII and forward to the DHA Privacy Office mailbox at: [DHA.PrivacyOfficer@mail.mil](mailto:DHA.PrivacyOfficer@mail.mil) for further action(s). Upon receipt, the DHA Privacy Office will review, advise, and direct appropriate mitigation and notification actions under the Privacy Act and HIPAA requirements.

The DHA Privacy Office is responsible for workforce members, to include the DHA Markets, MTFs, and headquarters, ensuring compliance with federal laws and DoD issuances with respect to breaches involving PII and PHI maintained by the MHS.



### 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>

**Preparing For and Responding to a Breach of Personally Identifiable Information**

Office of Management and Budget M-17-12, January 3, 2017

# MILITARY COMMAND EXCEPTION

## Disclosing Protected Health Information (PHI) of Armed Forces Personnel

In accordance with the HIPAA Privacy Rule, DoD Manual (DoDM) 6025.18, *Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs*, March 13, 2019 and applicable DoD issuances, a DoD covered entity (CE) may use and disclose the PHI of Armed Forces personnel 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.” Reference Paragraph 4.4.k.(1)(b) of the DoDM 6025.18 for further information on “appropriate military command authorities.”

This exception explains when DoD healthcare providers may disclose Service members’ PHI to military commanders for authorized uses (e.g., evaluating fitness for duty). If the specific requirements of this exception are satisfied, the Service member’s authorization is not required prior to a provider making the disclosure to a command authority. Note, the HIPAA Privacy Rule only permits DoD providers to disclose PHI under the military command exception, the Rule does not require such disclosures. While non-DoD providers and other CEs are not required to abide by DoDM 6025.18, the exception is still applicable to private hospitals and physicians as stated in the HIPAA Privacy Rule (reference 45 Code of Federal Regulations (CFR) 164.512(k)(1)(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.*



### MILITARY COMMAND AUTHORITY DEFINITION

- 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 authorized 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.

## ACCOUNTING OF DISCLOSURES

Disclosures to military commanders must be documented for disclosure accounting purposes (reference DoDM 6025.18 for guidance). The Protected Health Information Management Tool (PHIMT) is available for MHS CEs to document such disclosures made under the military command exception and the time those disclosures are made.



### PHIMT ASSISTANCE

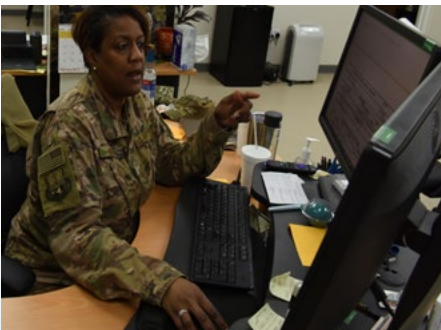
For PHIMT assistance, visit:  
<http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Act-and-HIPAA-Privacy-Training>



## MENTAL HEALTH AND/OR SUBSTANCE 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 1.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.

### **i** 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 Enclosure 2, Subparagraphs 1.b.(1) through 1.b.(9) of DoDI 6490.08. 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.

## 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 disclosure accounting requirements and methods for documenting disclosures

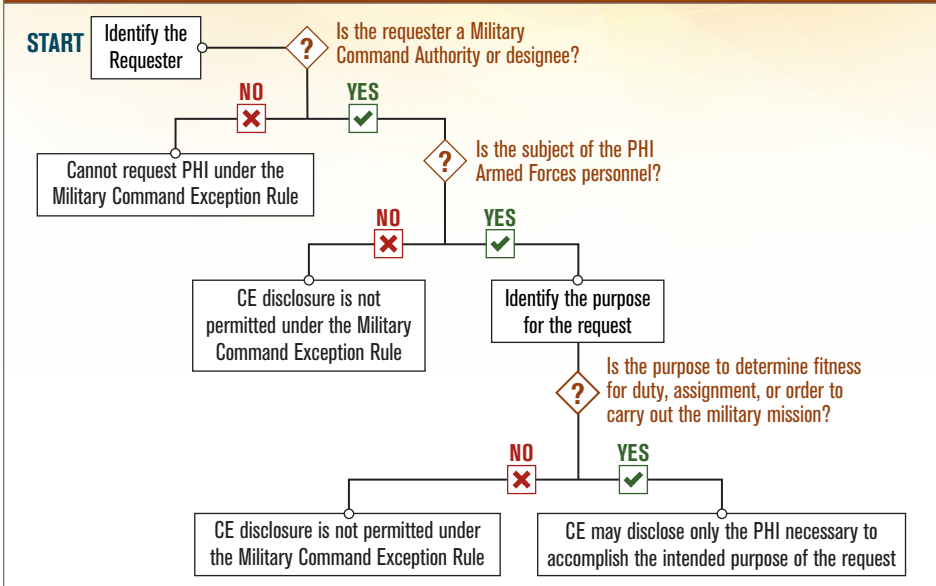
### WHAT IS "NECESSARY TO ASSURE PROPER EXECUTION OF THE MILITARY MISSION?"

Under Paragraph 4.4.k.(c) of DoDM 6025.18, 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 1332.18, *Disability Evaluation System (DES)*, August 5, 2014 (incorporating Change 1, May 17, 2018), and
  - DoDI 5210.42, *DoD Nuclear Weapons Personnel Reliability Assurance*, April 27, 2016 (incorporating Change 2), August 31, 2018
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



## PLANS FOR TRANSITION

The National Defense Authorization Act of 2017 organized the administrative control and transition of the Service MTFs' (i.e. Air Force, Army, and Navy) realignment to DHA. To ensure DHA incorporated all of the activities which affect the MTFs and their primary and sub-organizations, the DHA Privacy Office established several working groups that discussed a variety of issues which affected the posture of the MTFs and their organizations thereof. The Military Exception allows Military and civilian MTFs to use and disclose the PHI of an active duty member without authorization for activities deemed necessary by the active duty member's commander or a unit

command official designated by the commander. This includes: to ensure proper execution of the military mission, and to determine the active duty member's fitness for duty. When designed, the DHA Privacy Office Military Exception Training will help educate:

- MTF Commanders and Senior Leadership (Directors, Chiefs of Staff, etc.)
- MTF Primary and sub-organization level Privacy Officers, Privacy Liaisons, etc.
- Market Privacy Liaisons
- DHA Workforce members, as required



## POINT OF CONTACT

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



## RESOURCES

**Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs**  
DoDI 6025.18, March 13, 2019

**Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs**  
DoDM 6025.18, March 13, 2019

**DoD Privacy Program**  
DoD 5400.11-R, May 14, 2007  
DoDI 5400.11, January 29, 2019

**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

## The MHS GENESIS Roll Out Continues

Market dynamics and government action continue to transform the healthcare market. The Health Information Technology for Economic and Clinical Health Act provides incentives to increase the adoption of electronic health records (EHRs). As a result, EHRs have served as a major technology catalyst by providing the foundational data storage for massive amounts of information. Although the details must 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 MHS GENESIS Full Deployment Decision on November 28, 2018, DoD took another bold step in response to the transforming healthcare market. MHS GENESIS will eventually replace the Armed Forces Health Longitudinal Technology Application, Essentris®, and the Composite Health Care System 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 (IT) infrastructure so that 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.

### VA TO USE MHS GENESIS

The VA has decided to replace the Veterans Information Systems and Technology Architecture with MHS GENESIS. This decision dramatically increases the amount of data requiring safeguards, and perhaps more significantly, impacts the relationship between VA and DoD. This is done by requiring alignment of technical capabilities, policies, and operational support as well as stakeholder agreement on legal and compliance issues. Go-live for the VA launch in July 2020 marks the initial step in managing the health data of approximately 23.5 million veterans under the MHS GENESIS system.



### THE IMPACT OF NEW SYSTEMS AND MOBILE TECHNOLOGIES

The rapid introduction of new technologies raises 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 many years and while complicated, are well understood by specialized individuals assigned to assess whether they have been granted.

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 challenges to the military. 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 (PHI) 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.



## HEALTH INFORMATION EXCHANGE

The Joint Legacy Viewer is the primary viewer used by the MHS and enables DoD and the VA to view health data from military treatment facilities (MTFs) and participants in the eHealth Exchange. eHealth Exchange participants include the VA, private partners, and other federal and state organizations. Data exchanged through the eHealth Exchange is governed by the Data Use and Reciprocal Support Agreement, which is being updated to reflect changes to federal contracting requirements and Controlled Unclassified Information (CUI) regulations. CUI includes both PHI and personally identifiable information (PII).



### PLANS FOR TRANSITION

With the full implementation of the National Defense Authorization Act of 2017, DHA will ultimately assume responsibility for most MTF-owned systems as system approval and oversight will no longer be the responsibility of the Services. The scope of oversight will include medical devices and systems with interfaces to MHS GENESIS. The DHA Privacy Office will play a major role in ensuring systems processing PII and PHI meet privacy requirements. In preparation for these changes, the DHA Privacy Office is establishing close working relationships with local IT personnel and the DHA Health Information Technology Division to ensure privacy-compliant systems.



## 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>

### **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs**

DoD Instruction (DoDI) 6025.18, March 13, 2019

### **Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs**

DoD Manual 6025.18, March 13, 2019

### **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**

DoDI 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 9/11 Commission 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 CLO to

oversee compliance. The DHA Privacy Office Chief has been designated by the DHA Director as the DHA CLO.

A component civil liberties program has several 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 culture of civil liberties awareness and compliance

Per DHA Administrative Instruction (AI) 64, DHA Civil Liberties Program, it is DHA policy to protect the privacy and civil liberties of all DHA employees, Service members, family members, and the public with whom they interact, 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.

### 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.

**Civil Liberties** – Offer protection to individuals from improper government action and arbitrary government interference. They are the freedoms guaranteed by the Bill of Rights – the first 10 Amendments to the 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.

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



### CIVIL LIBERTIES TODAY

A recently declassified 2018 ruling by the Foreign Intelligence Surveillance Court (the Court) determined that a Federal Bureau of Investigations (FBI) program, which monitors foreign suspects, violated tens of thousands of United States citizens' constitutional rights to privacy. The Court ruled that between 2017 and 2018, the FBI illegally collected personal information, including e-mails and telephone numbers of private United States citizens. Federal law restricts such database queries to those that are related to evidence of a crime or foreign intelligence. Here, the Court determined that the FBI's program procedures were contradictory to the right against unreasonable searches and seizures guaranteed by the Fourth Amendment.



## 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:

|                          |  |
|--------------------------|--|
| <b>First Amendment</b>   | Freedom of speech, religion, press, peaceful assembly, and the right to petition the government for a redress of grievances                                  |
| <b>Second Amendment</b>  | Right to bear arms   |
| <b>Third Amendment</b>   | Right not to have soldiers quartered in private residences without the consent of the owner  |
| <b>Fourth Amendment</b>  | Freedom against unreasonable searches and seizures   |
| <b>Fifth Amendment</b>   | Right against self-incrimination and to not be deprived of life, liberty, or property, without due process   |
| <b>Sixth Amendment</b>   | Right to a speedy trial  |
| <b>Seventh Amendment</b> | Right to a trial by jury in cases over twenty dollars  |
| <b>Eighth Amendment</b>  | Freedom from cruel and unusual punishment  |
| <b>Ninth Amendment</b>   | Protects “non-enumerated rights” (e.g., right to travel, right to a presumption of innocence)  |
| <b>Tenth Amendment</b>   | The reservation of “States’ Rights” – This Amendment makes it explicit that the Federal Government is limited only to the powers granted in the Constitution |



## PLANS FOR TRANSITION

As the DHA Privacy Office continues transition efforts under the National Defense Authorization Act of 2017, it will expand its DoD recognized Civil Liberties Program to serve as the oversight program for all military treatment facilities (MTFs) within the DoD.

Under this comprehensive Civil Liberties Program, each MTF will designate a Privacy Liaison to adjudicate Civil Liberties complaints. This will include reporting all complaints to the DHA Privacy Office; conducting investigations in collaboration with necessary resources including, but not limited to, the organization's Legal and Human Resources departments; and drafting a final report on its findings, which must be sent to the DHA Privacy Office for final resolution.

The DHA Privacy Office will continue to identify and collaborate with appropriate leadership to create awareness and provide education and training on its Civil Liberties Program to MTFs, while determining best practices to advance outreach to impacted stakeholders.



## 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 Privacy and Civil Liberties Program**

DoD Instruction (DoDI) 5400.11, January 29, 2019

### **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

### **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs**

DoDI 6025.18, March 13, 2019

### **Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs**

DoD Manual 6025.18, March 13, 2019

### **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 that was enacted in 1966 granting 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 (in this chapter). 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 of the United States 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 limit 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. Additionally, requests requiring more than 20 days to process are classified as complex requests.

**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.

**Multi-track Processing** – A system that divides incoming FOIA requests according to their complexity so that simple requests requiring relatively minimal research and review are placed in one processing track and more complex requests are placed in other track(s).

**“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.

**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.

## 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 memoranda 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

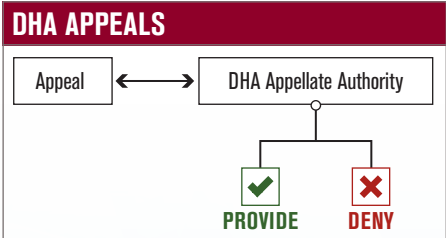
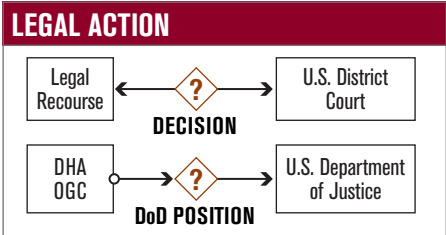
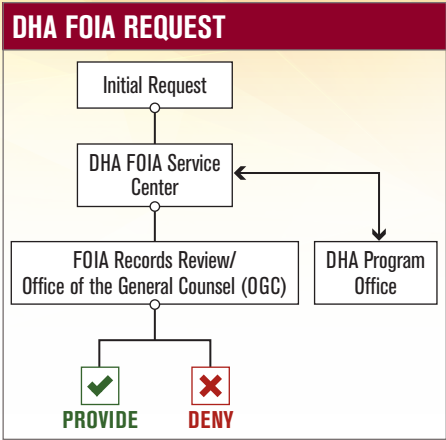
**Pending Request or Pending Administrative Appeal** – A FOIA request or administrative appeal for which an agency has not taken final action in all respects.

**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.

**Referral** – When an agency locates a record that originated with, or is of otherwise primary interest to another agency, it will forward that record to the other agency to process that record and to provide the final determination directly to the requester.

**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 (FOIA-SC) processes both FOIA requests and Privacy Act requests for the DHA. If a workforce member receives requests for information, please contact the DHA FOIA-SC using the following information: 703-275-6017 or [DHA.FOIA@mail.mil](mailto:DHA.FOIA@mail.mil).

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



## PLANS FOR TRANSITION

Since 2018, the DHA Privacy Office has engaged in regular meetings and workgroups to collaborate with the Services in creating a joint implementation strategy. In light of transition, the DHA FOIA-SC will become the MHS FOIA-SC, which has also met regularly with other civilian and military stakeholders to discuss best practices for the phased transitions ahead.

To accomplish DoD’s proposed implementation plan as it pertains to the FOIA Program, DHA has planned to establish the MHS FOIA-SC as the official processing hub for all FOIA and Privacy Act disclosure requests on behalf of the military treatment facilities (MTFs), while planning to launch one or more Satellite Processing Centers based on unique request types. The DHA has also planned to require each MTF and/or Market to have a Privacy Liaison that serves as a point of contact for FOIA searches and Privacy Act disclosures and report back to MHS FOIA-SC for processing. Lastly, the DHA will reconstruct the FOIA library at [www.health.mil](http://www.health.mil) to meet proactive disclosure requirements and make record searches initiated by the general public more user-friendly and ultimately serve as a comprehensive FOIA library.





## 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 Library

<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](http://www.usdoj.gov/oip/amendment-s2488.pdf)

### 32 United States Code of Federal Regulations Part 286

<https://www.federalregister.gov/documents/2017/01/05/2016-31686/dod-freedom-of-information-act-foia-program>

### DoD Freedom of Information Act (FOIA) Program

DoD 5400.7, January 25, 2017

### DoD Privacy Program

DoD 5400.11-R, May 14, 2007

DoD Instruction 5400.11, January 29, 2019

### FOIA Improvement Act of 2016

<https://www.congress.gov/bill/114th-congress/senate-bill/337>









MEDICAL

Health Care  
Doctor  
Hospital  
Pharmacy  
Nurse  
Dentist  
Specialist  
Surgeon  
Emergency

