



## DoD INSTRUCTION 6025.18

# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE COMPLIANCE IN DoD HEALTH CARE PROGRAMS

---

<b>Originating Component:</b>	Office of the Under Secretary of Defense for Personnel and Readiness
<b>Effective:</b>	March 13, 2019
<b>Releasability:</b>	Cleared for public release. This instruction is available on the Directives Division Website at <a href="http://www.esd.whs.mil/DD/">http://www.esd.whs.mil/DD/</a> .
<b>Reissues and Cancels:</b>	DoD Instruction 6025.18, "Privacy of Individually Identifiable Health Information in DoD Health Care Programs," December 2, 2009
<b>Approved by:</b>	James N. Stewart, Assistant Secretary of Defense for Manpower and Reserve Affairs, Performing the Duties of the Under Secretary of Defense for Personnel and Readiness

---

**Purpose:** This issuance, in accordance with the authority in DoD Directive 5124.02, establishes policy and assigns responsibilities for:

- DoD compliance with federal law governing health information privacy and breach of privacy.
- Integrating health information privacy and breach compliance with general information privacy and security requirements in accordance with federal law and DoD issuances.
- Health information technology, system interoperability, and exchange of electronic health information, in relation to federal law governing health information privacy and breach.
- DoD contracting and procurement activities in relation to federal law governing health information privacy and breach.

## TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION .....	3
1.1. Applicability. ....	3
1.2. Policy. ....	3
SECTION 2: RESPONSIBILITIES .....	5
2.1. Assistant Secretary of Defense for Health Affairs (ASD(HA)).....	5
2.2. Director, DHA.....	5
2.3. Secretaries of the Military Departments. ....	5
GLOSSARY .....	6
G.1. Acronyms. ....	6
G.2. Definitions.....	6
REFERENCES .....	8

## SECTION 1: GENERAL ISSUANCE INFORMATION

### 1.1. APPLICABILITY. This issuance applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the “DoD Components”).

b. Certain elements of the U.S. Coast Guard as in accordance with DoD Manual (DoDM) 6025.18.

c. DoD covered entities and their business associates. These DoD covered entities and their business associates are regulated in accordance with federal regulations issued by the Department of Health and Human Services (HHS) pursuant to Public Law 104-191 as amended, also known and referred to in this issuance as “HIPAA.” This issuance, together with DoDM 6025.18, as applied to DoD covered entities and their business associates, implements the HIPAA regulations in DoD.

### 1.2. POLICY. It is DoD policy that:

a. DoD covered entities and business associates:

(1) Must follow the HIPAA Privacy and Breach Rules and their implementation in DoD in accordance with DoDM 6025.18.

(2) Must comply with related federal requirements otherwise applicable to them as federal and DoD entities. Therefore, this issuance applies in conjunction with:

(a) Section 552a of Title 5, United States Code, as amended (also known and referred to in this issuance as “The Privacy Act”), and DoD Privacy Act issuances, which establish policy regarding the privacy of personally identifiable information (including but not limited to protected health information (PHI), if the information pertains to a living U.S. citizen or alien admitted for permanent residence.

(b) Federal rules protecting the confidentiality of patient records in federally assisted substance use disorder programs in accordance with DoDM 6025.18.

(c) DoD cybersecurity requirements.

(d) Applicable DoD issuances and DoD Component publications affecting the management of records maintained by a DoD covered entity.

(3) Must, as authorized by and consistent with the procedures pursuant to DoDM 6025.18, ensure the availability to appropriate command authorities of health information

concerning military personnel necessary to ensure the proper execution of the military mission. In doing so, DoD covered entities and business associates must follow the policies regarding mandatory and prohibited releases of PHI pursuant to DoD Instruction 6490.08 to dispel stigma associated with seeking mental health services, substance misuse education services, or both.

(4) Will dispose of or destroy records containing PHI in accordance with this issuance and applicable DoD, Defense Health Agency (DHA) component, or Service authorized records disposition authorities.

b. DHA and Service-level contracting policies and procedures for health services contracts and other medical and dental support, information technology contracts, and other DoD procurement activities pertaining to investments in health information technology must remain in accordance with this issuance, DoDM 6025.18, and additional guidance from DoD and HHS regarding the HIPAA Privacy Rule.

c. DoD must foster the development and expansion of health information system interoperability, the electronic exchange of PHI, and electronic health record system development and policy, in a manner that provides reasonable safeguards for the confidentiality, integrity, and availability of PHI created, received, maintained, or transmitted through electronic media.

## SECTION 2: RESPONSIBILITIES

### 2.1. ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS (ASD(HA)).

Under the authority, direction, and control of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), the ASD(HA):

- a. Oversees compliance with this issuance, in accordance with the Privacy Act, other applicable federal law and agency guidance, and DoD guidance pertaining to information privacy, data security, and records management, as well as current and future HHS guidance in accordance with the HIPAA Privacy and Breach Rules.
- b. Delegates authority to DHA to develop and update supporting guidance in accordance with this issuance as necessary.
- c. Proposes modifications of this issuance to the USD(P&R), after coordination of recommendations originating from the Director, DHA, or other DoD Components as necessary or required.

### 2.2. DIRECTOR, DHA. Under the authority, direction, and control of the USD(P&R), through the ASD(HA), the Director, DHA:

- a. Oversees DoD covered entities and business associates within the DHA, as well as applicable activities of the DoD Components throughout the Military Health System, to ensure compliance with this issuance.
- b. Coordinates, as appropriate, with the Defense Privacy, Civil Liberties, and Transparency Division regarding the Privacy Act and other applicable federal law and agency guidance within the division's purview.
- c. Oversees coordination between the DHA Privacy Office and the DHA Office of Chief Information Officer/Health Information Technology Directorate to ensure that interoperability, electronic information exchange, and PHI access rights of individuals are consistent with the HIPAA Privacy Rule.
- d. Develops and proposes modifications to this issuance and prepares supporting guidance when warranted by regulatory changes; DoD, DHA, or Military Health System governance changes; operational experience; DoD Component input; or reconsideration of the provisions of this issuance. Future development may address policies and procedures for different categories of PHI in recognition that not all PHI has equal sensitivity in all circumstances.

### 2.3. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments oversee DoD covered entities and business associates within the Military Services to ensure compliance with this issuance.

## GLOSSARY

### G.1. ACRONYMS.

ASD(HA)	Assistant Secretary of Defense for Health Affairs
DHA	Defense Health Agency
DoDM	DoD Manual
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
PHI	protected health information
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

### G.2. DEFINITIONS. These terms and their definitions are for the purpose of this issuance.

**business associate.** With respect to a DoD covered entity, a party that creates, receives, maintains, or transmits PHI on behalf of the DoD covered entity for a function or activity regulated by this issuance; or a party that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such DoD covered entity, where the provision of the service involves disclosure of PHI to that party. A DoD or other covered entity may be a business associate performing HIPAA-covered functions on behalf of another DoD covered entity. A more detailed definition is provided in DoDM 6025.18.

**covered entity.** A health plan, or a health care provider who transmits any health information in electronic form in connection with a standard transaction pursuant to Part 162 of Title 45, Code of Federal Regulations. A more detailed definition is provided in DoDM 6025.18.

**DoD covered entity.** In the case of a health plan administered by DoD, the DoD Component (or subcomponent) functions as the administrator of the health plan. To the extent this issuance prescribes duties to be performed by covered entities, the term refers only to DoD covered entities. All covered entities within the Military Health System (including both health plans and health care providers) are DoD covered entities and designated as a single covered entity. Not all health care providers affiliated with the Military Services are DoD covered entities; among those who are not are:

Providers associated with military entrance processing stations or DoD medical examination review boards.

Reserve Components practicing outside the authority of military treatment facilities that do not engage in electronic standard transactions covered by this issuance.

A more detailed definition is provided in DoDM 6025.18.

**DoD cybersecurity requirements.** Current DoD issuances and other federal law relating to electronic data security and protection of DoD information systems. A more detailed definition is provided in DoDM 6025.18.

**DoD Privacy Act issuances.** DoD issuances implementing the Privacy Act of 1974 in DoD.

**employment records.** Records about an individual who is (or seeks or sought to become) a member of the uniformed services, employee of the U.S. Government, employee of a DoD contractor, or person with a comparable relationship to the DoD, that are maintained by a DoD Component or other entity subject to this issuance. A more detailed definition is provided in DoDM 6025.18.

**HIPAA Privacy Rule.** The HIPAA Rule governing the use and disclosure of PHI held by covered entities and business associates.

**HIPAA Rules.** The rules and instructions issued by HHS pursuant to Section 264(c) of HIPAA and captioned the HIPAA Privacy, Security, Breach, and Enforcement Rules (see the References). This term does not include the HIPAA transaction, code set, and identifier rules in Part 162 of Title 45, Code of Federal Regulations.

**Military Health System.** All DoD health plans and all DoD health care providers that are, in the case of institutional providers, organized in accordance with the management authority of, or in the case of covered individual providers, assigned to or employed by, the DHA, the Surgeon General of the Army, the Surgeon General of the Navy, or the Surgeon General of the Air Force.

**PHI.** Individually identifiable health information (as defined in the HIPAA Privacy Rule) that, except as provided in this issuance, is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a DoD covered entity in its role as employer. Information that has been de-identified in accordance with the HIPAA Privacy Rule is not PHI.

**personally identifiable information.** Defined in DoD Directive 5400.11. PHI is a subset of personally identifiable information, with respect to living individuals.

## **REFERENCES**

- Code of Federal Regulations, Title 45, Parts 160 and 162, as amended<sup>1</sup>
- DoD Directive 5124.02, “Under Secretary of Defense for Personnel and Readiness (USD(P&R)),” June 23, 2008
- DoD Instruction 5400.11, “DoD Privacy and Civil Liberties Program,” January 29, 2019
- DoD Instruction 6490.08, “Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members,” August 17, 2011
- DoD Manual 6025.18, “Implementation of the HIPAA Privacy Rule in DoD Health Care Programs,” March 13, 2019
- Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996,” August 21, 1996, as amended (also known and referred to in this issuance as “HIPAA”)
- United States Code, Title 5, Section 552a, as amended (also known and referred to in this issuance as “The Privacy Act”)

---

<sup>1</sup> Part 164, Subpart E is also known as the HIPAA Privacy Rule.  
Part 164, Subpart D is also known as the HIPAA Breach Rule.  
Part 164, Subpart C is also known as the HIPAA Security Rule  
Part 160, Subparts C, D, and E is also known as the HIPAA Enforcement Rule.  
The definitions and certain other provisions in Part 160, Subpart A apply to all four of the Rules.