



DoD MANUAL 6025.18

IMPLEMENTATION OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE IN DoD HEALTH CARE PROGRAMS

Originating Component:	Office of the Under Secretary of Defense for Personnel and Readiness
Effective:	March 13, 2019
Releasability:	Cleared for public release. This manual is available on the Directives Division Website at http://www.esd.whs.mil/DD/ .
Reissues and Cancels:	DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
Approved by:	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 (DoDD) 5124.02, implements the policy in DoD Instruction (DoDI) 6025.18, assigns responsibilities, and provides procedures for:

- DoD compliance with the privacy regulations adopted under HIPAA, Public Law 104-191, at:
 - Part 160 and Part 164, Subpart E of Title 45, Code of Federal Regulations (CFR) (also known and referred to in this issuance as the "HIPAA Privacy Rule").
 - Part 160 and Part 164, Subpart D of Title 45, CFR (also known and referred to in this issuance as the "HIPAA Breach Rule").
- Integration of HIPAA compliance with related information privacy and security requirements, health information technology development, and associated procurement activities.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION	6
1.1. Applicability.	6
1.2. Policy.	7
1.3. Information Collections.	8
SECTION 2: RESPONSIBILITIES	9
2.1. Director, DHA.....	9
2.2. DoD Component Heads of DoD Covered Entities.	9
SECTION 3: AUTHORITIES, SCOPE, ENFORCEMENT, OTHER LAWS, AND ORGANIZATIONAL RESPONSIBILITIES	11
3.1. Legal Authorities in General.....	11
a. General Provisions.	11
b. Uses and Disclosures of PHI.....	11
c. Uses and Disclosures of PHI Special Rules and Requirements.....	12
d. DoD Covered Entity Obligations Regarding Individual Rights.	13
e. Breach Response Provisions.	13
f. Additional Administrative Requirements for the MHS to Implement Health Information Privacy Protections.	13
3.2. Scope, Enforcement, and Relationship to Other Laws.	14
a. Inspector General.	14
b. Preemption of State Law.....	14
c. Compliance and Enforcement by the Secretary of HHS.....	15
d. Relationship to the Privacy Act.	18
e. No Private Cause of Action.....	18
f. Relationship to Section 552 of Title 5, U.S.C., Also Known as the “Freedom of Information Act (FOIA).”	18
3.3. Organizational Roles and Responsibilities.	19
a. Covered Entities in the MHS.	19
b. The MHS and Organized Health Care Arrangements.	20
c. Business Associate Arrangements among and for DoD Components.	21
d. Requirements for a Covered Entity with Multiple Covered Functions.	24
e. DoD as a Hybrid Entity.....	24
SECTION 4. USES AND DISCLOSURES OF PHI.....	25
4.1. General Rules on Uses or Disclosures of PHI.	25
a. Standard: Permitted and Prohibited Uses and Disclosures.	25
b. Implementation Specifications: Treatment, Payment, and Health Care Operations. .	25
c. Implementation Specifications: Disclosures through Health Information Exchange.	26
4.2. Uses And Disclosures for Which an Authorization Is Required.	26
a. Standard Operating Procedures.....	26
b. Implementation Specifications: General Requirements.....	28
c. Implementation Specifications: Core Elements and Requirements.....	30
4.3. Uses and Disclosures Requiring an Opportunity for Individual to Agree or to Object..	31
a. Standard: Use and Disclosure for Facility Directories.....	32

b. Standard: Uses and Disclosures for Involvement in the Individual’s Care and Notification Purposes.....	33
4.4. Uses and Disclosures for Which an Authorization or Opportunity to Agree or Object Is Not Required.....	34
a. Standard: Uses and Disclosures Required by Law.....	34
b. Standard: Uses and Disclosures for Public Health Activities.....	35
c. Standard: Disclosures About Victims of Abuse, Neglect, or Domestic Violence.....	36
d. Standard: Uses and Disclosures for Health Oversight Activities.....	37
e. Standard: Uses and Disclosures for Judicial and Administrative Proceedings.....	39
f. Standard: Disclosures for Law Enforcement Purposes.....	41
g. Standard: Uses and Disclosures About Decedents.....	43
h. Standard: Uses and Disclosures for Cadaveric Organ, Eye, or Tissue Donation Purposes.....	43
i. Standard: Uses and Disclosures for Research Purposes.....	43
j. Standard: Uses and Disclosures to Avert Serious Threat to Health or Safety.....	46
k. Standard: Uses and Disclosures for Specialized Government Functions.....	47
l. Standard: Disclosures for Workers Compensation.....	50
4.5. Special Rules and Other Requirements Relating to Uses And Disclosures of PHI.....	50
a. De-Identification of PHI.....	50
b. Minimum Necessary Rule.....	52
c. Limited Data Set.....	54
d. Incidental Use and Disclosure Rule.....	56
e. Standard: Disclosure to Business Associates.....	57
f. Standard: Disclosures by Whistleblowers and Workforce Crime Victims.....	57
g. Personal Representatives.....	58
h. Standard: Deceased Individuals.....	60
i. Verification of Identity Before Disclosure of PHI.....	60
j. Special Rules for Substance Use Disorder Records.....	62
k. Special Rules for Genetic Information.....	62
SECTION 5. RIGHTS OF INDIVIDUALS.....	63
5.1. Notice of Privacy Practices (NoPP) for PHI.....	63
a. Standard: NoPP.....	63
b. Implementation Specifications: Content of MHS NoPP.....	63
c. Implementation Specifications: Provision of MHS NoPP.....	63
d. Implementation Specifications: Joint Notice by Separate Covered Entities.....	65
e. Implementation Specifications: Documentation.....	65
5.2. Rights to Request Privacy Protection for PHI.....	65
a. Right to Request Restriction.....	65
b. Right to Request Confidential Communications.....	67
5.3. Access of Individuals to PHI.....	68
a. Standard: Access to PHI.....	68
b. Implementation Specifications: Requests for Access and Timely Action.....	70
c. Implementation Specifications: Provision of Access.....	70
d. Implementation Specifications: Denial of Access.....	72
e. Implementation Specifications: Documentation.....	73

5.4. Amendment of PHI	73
a. Standard: Right to Amend.....	73
b. Implementation Specifications: Requests for Amendment and Timely Action.	73
c. Implementation Specifications: Accepting the Amendment.....	74
d. Implementation Specifications: Denying the Amendment.	74
e. Implementation Specifications: Actions on Notices of Amendment.....	76
f. Implementation Specifications: Documentation.	76
g. Relationship to the Privacy Act.	76
5.5. Accounting of Disclosures of PHI.....	76
a. Standard: Right to an Accounting of Disclosures of PHI.	76
b. Implementation Specifications: Content of Accounting.....	77
c. Implementation Specification: Provision of Accounting.....	78
d. Implementation Specification: Documentation.	79
e. Relationship to the Privacy Act.....	79
SECTION 6: BREACH RESPONSE.....	80
6.1. Breach Response Obligations.	80
a. Requirement.	80
b. DHA Privacy Office Roles and Authority.....	80
6.2. Breach Response Procedures.	81
a. Overview.....	81
b. Initial Reporting.....	81
c. Assessments.....	81
d. Individual Notification.....	81
e. Media Notification.....	82
f. Reporting to Secretary of HHS.....	83
g. Special Rules.....	83
h. Documentation.....	84
6.3. Breach Risk Analysis Template.....	85
a. Risk analysis.....	85
b. Updates to template.....	85
SECTION 7: ADMINISTRATIVE AND TRANSITION PROVISIONS.....	87
7.1. Personnel Requirements.....	87
a. Personnel Designations.....	87
b. Training.....	87
c. Sanctions.....	88
7.2. Protections for Individuals and Others.	89
a. Complaints.....	89
b. Standard: Refraining from Intimidating or Retaliatory Acts.....	90
c. Standard: Waiver of Rights.....	90
7.3. Other Covered Entity Requirements.....	90
a. Safeguards.....	90
b. Standard: Mitigation.....	90
c. Policies and Procedures.....	90
d. Documentation.....	92
7.4. Compliance Dates and Transition Provisions.....	92

a. Standard: Effect of Prior Authorizations.....	92
b. Business Associate Arrangements and Data Use Agreements.	93
GLOSSARY	94
G.1. Acronyms.	94
G.2. Definitions.....	94
REFERENCES	109

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security (DHS) by agreement with that Department), 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”).

(a) Within the DoD Components, this issuance applies to the following as DoD covered entities under the HIPAA Privacy Rule: all DoD health plans and all DoD health care providers that engage in electronic standard transactions and that are, in the case of institutional health care providers, organized under the management authority of, or in the case of covered individual health care providers, assigned to or employed by, the Defense Health Agency (DHA), the Department of the Army, the Department of the Navy, or the Department of the Air Force (referred to collectively in this issuance as “DoD covered entities”).

(b) Not all institutional health care providers or individual health care providers affiliated with the Military Services are DoD covered entities.

(c) This issuance applies to DoD Components when acting as HIPAA business associates.

(d) In addition to DoD Components, this issuance also applies to certain elements of the U.S. Coast Guard, as provided in Paragraph 3.3.(b)(1)-(2).

(2) Non-DoD government agencies and Military Health System (MHS) contractors that meet the definition of a business associate with respect to the protected health information (PHI) of a DoD covered entity where the contract or other written arrangement makes this issuance or DoDI 6025.18 applicable.

b. This issuance does **not** apply to:

(1) A DoD drug testing program carried out under the authority of DoDI 1010.01 or DoDI 1010.09.

(2) The provision of health care to foreign national beneficiaries of the MHS when such care is provided in a country other than the United States.

(3) The Armed Forces Repository of Specimen Samples for the Identification of Remains.

(4) The provision of health care to enemy prisoners of war, retained personnel, civilian internees, and other detainees under the provisions of DoDD 2310.01E.

(5) Education records maintained by domestic or overseas schools operated by the DoD.

(6) Records maintained by day care centers operated by the DoD.

(7) Military Entrance Processing Stations.

(8) DoD Medical Examination Review Board.

(9) Armed Forces Medical Examiner System.

(10) Armed Forces Health Surveillance Branch.

(11) Reserve and National Guard component medical personnel who are outside the authority of the military treatment facilities (MTFs) and do not engage in electronic standard transactions covered by this issuance.

(12) Health care providers participating in the provider networks of DHA managed care support contractors, except to the extent that the agreements between such contractors and providers apply this issuance to such providers.

1.2. POLICY.

a. In accordance with Paragraph 1.2.a.(1) of DoDI 6025.18, DoD covered entities and business associates must follow the HIPAA Privacy and Breach Rules as implemented in this issuance.

b. In accordance with Paragraph 1.2.a.(2) of DoDI 6025.18, DoD covered entities and business associates must comply with requirements applicable to federal entities, relating to:

(1) Section 552a of Title 5, United States Code (U.S.C.), also known as and referred to in this issuance as the "Privacy Act," as amended; and DoD Privacy Program issuances, including DoD 5400.11-R.

(2) Federal rules protecting the confidentiality of patient records in federally assisted substance use disorder programs.

(3) DoD cybersecurity requirements.

(4) Applicable DoD and DoD Component issuances affecting the management of records maintained by or for a DoD covered entity.

c. In accordance with Paragraphs 1.2.a.-c. of DoDI 6025.18, DoD covered entities and business associates must also follow the policies, as implemented by this issuance, relating to:

(1) Military command authorities and the need to dispel stigma associated with seeking mental health services and substance misuse education services.

(2) Contracting policies and procedures.

(3) Health information system interoperability, the electronic exchange of PHI, and electronic health record system technology development and clinical policy.

(4) Records retention and destruction requirements.

1.3. INFORMATION COLLECTIONS.

a. The breach response reporting requirement, referred to in Paragraph 2.2.b. and Section 6, does not require licensing with a report control symbol in accordance with Paragraph 1.b.(8) of Volume 1 of DoD Manual 8910.01.

b. The compliance reports, referred to in Paragraphs 2.2.c.(3) and 3.2.c.(4)(a), do not require licensing with a report control symbol in accordance with Paragraph 1.b.(8) of Volume 1 of DoD Manual 8910.01.

c. The complaints to the Department of Health and Human Services (HHS), referred to in Paragraphs 3.2.c.(2) and 7.2.a., do not require licensing with a report control symbol in accordance with Paragraph 1.b.(8) of Volume 1 of DoD Manual 8910.01.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DHA. Under the authority, direction, and control of the Under Secretary of Defense for Personnel and Readiness, through the Assistant Secretary of Defense for Health Affairs (ASD(HA)), the Director, DHA:

a. Oversees DoD covered entities' implementation of DoDI 6025.18 to foster the development and expansion of health information system interoperability, the electronic exchange of PHI, and electronic health record system management, in a manner that provides reasonable safeguards for the confidentiality, integrity, and availability of PHI created, received, maintained, or transmitted through electronic media.

b. Acts as the proponent for implementation of the HIPAA rules by issuing guidance to the MHS and DHA or preparing guidance for the MHS and DHA to be issued by the Office of the ASD(HA) or DHA, as appropriate, taking into account relevant HHS guidance. Such MHS and DHA guidance may also be issued through the DHA Privacy Office. Guidance issued through the DHA Privacy Office will be made effective as of its posting to the DHA Privacy Office Website or the DHA Publications Website, as appropriate.

c. Appoints a HIPAA Privacy and Security Officer for DHA.

d. Through the Chief, DHA Privacy Office:

(1) Issues guidance to the MHS and acts as the proponent for HIPAA implementation through this issuance, taking into account HHS guidance. Guidance issued by the DHA Privacy Office will be made effective as of its posting to the DHA Privacy Office Website or the DHA Publications website, as appropriate.

(2) Coordinates with the DHA Chief Information Officer and other appropriate officials with regard to the Director, DHA, responsibility to effectively integrate implementation of the HIPAA Privacy Rule with DoD cybersecurity requirements, health information system interoperability, electronic information exchange, individuals' access to their PHI and communications with their providers, and related contracting matters.

(3) Recommends to the Director, DHA, proposed changes to this issuance or other new guidance when warranted by regulatory changes; DoD, DHA, or MHS governance changes; operational experience; or reconsideration of the provisions of this issuance.

2.2. DOD COMPONENT HEADS OF DOD COVERED ENTITIES. The DoD Component heads of DoD covered entities:

a. Fulfill the rights of individuals concerning PHI as provided in Section 5.

b. Carry out breach response requirements in the event of a breach of PHI as provided in Section 6.

c. Perform the personnel and other administrative requirements necessary to implement health information privacy protections, including but not limited to:

(1) Designating a HIPAA privacy officer and a contact person or office for each DoD covered entity such as an MTF within the DoD Component. A DoD covered entity's HIPAA privacy officer may also be the designated HIPAA Security Officer for that DoD covered entity in accordance with in DoDI 8580.02.

(2) Maintaining records.

(3) Submitting compliance reports requested by HHS.

(4) Cooperating with complaint investigations and compliance reviews.

(5) Permitting access to information, as provided in Paragraphs 5.3. and 7.1. through 7.4.

d. Ensure contracts include requirements to protect DoD PHI, and are monitored for compliance.

e. Adhere to guidance from the Director, DHA; and the Chief, DHA Privacy Office, in carrying out the responsibilities as provided in this paragraph.

f. Monitor guidance provided by the DHA. This includes:

(1) All applicable guidance issued through the DHA Privacy Office, DHA Medical Record Management offices, and the DHA Chief Information Officer/Health Information Technology Directorate.

(2) Consultations with those offices as necessary to ensure that implementation of the HIPAA Privacy Rule is effectively integrated in accordance with Part 160 and Part 164, Subpart C of Title 45, CFR, also known and referred to in this issuance as the "HIPAA Security Rule," and other DoD cybersecurity requirements.

SECTION 3: AUTHORITIES, SCOPE, ENFORCEMENT, OTHER LAWS, AND ORGANIZATIONAL RESPONSIBILITIES

3.1. LEGAL AUTHORITIES IN GENERAL.

a. General Provisions.

(1) **Preemption of State Law.** Subject to the exceptions specified in Paragraph 3.2.b., this issuance applies to the activities of the MHS without regard to any contrary provision of State law.

(2) **Relationship with the Privacy Act.** In general, PHI covered by this issuance is also covered by the Privacy Act and the DoD Privacy Program issuances when the information pertains to a living U.S. citizen or alien lawfully admitted for permanent residence. As provided in Paragraph 3.2.d., DoD covered entities under this issuance must also comply with DoD Privacy Program issuances.

(3) **Other Matters of General Authority.** Other matters of general authority under this issuance are addressed in Paragraph 3.2.

b. Uses and Disclosures of PHI.

(1) **General Prohibition.** In general, PHI of individuals must not be used or disclosed by DoD covered entities or their business associates, except for specifically permitted or required purposes. Uses and disclosures of PHI are discussed in Paragraphs 4.1. through 4.5. This issuance applies to the PHI of living individuals and individuals deceased for fewer than 50 years.

(2) **Uses and Disclosures of PHI for Treatment, Payment, and Health Care Operations.** Subject to the specific provisions of Paragraphs 4.1. through 4.5., DoD covered entities may use and disclose PHI for treatment, payment, or health care operations. These activities are generally permitted, consistent with Paragraphs 4.1. through 4.5., to be conducted without the need for authorization from the subject of the PHI being used or disclosed, because these are essential, everyday activities of health plans and health care providers.

(3) **General Prohibition on Other Uses and Disclosures of PHI Without Written Authorization.** Except for purposes of treatment, payment, and health care operations (discussed in Paragraph 3.1.b.(2)) and other exceptions (discussed in Paragraphs 3.1.b.(3) through 3.1.b.(5)), other uses and disclosures of PHI are generally prohibited without the written authorization of the individual. Specific provisions pertaining to this general rule are addressed in Paragraph 4.2., including specifications for valid authorizations.

(a) **Special Rules for Psychotherapy Notes.** Paragraph 4.2.a.(2) establishes special rules that protect the privacy of psychotherapy notes even more so than other health information. Unless a use or disclosure of psychotherapy notes is specifically permitted by an exception in

Paragraph 4.2.a.(2), a use or disclosure of psychotherapy notes may only be made if the DoD covered entity obtains an authorization for such use or disclosure.

(b) **Special Rule for Genetic Information** Paragraph 4.5.k. establishes a special rule prohibiting health plans from using or disclosing PHI that is genetic information for underwriting, even if the affected individual has executed an authorization for such purposes.

(4) **Other Uses and Disclosures That Are Permissible Unless Objected To.** Individuals must be given an opportunity to object to uses and disclosures that involve patient directories providing limited information about patients receiving treatment; information provided to others involved in the health care of the patient; and information used for disaster relief purposes. The specific provisions applicable to these uses and disclosures are in Paragraph 4.3.

(5) **Other Permitted and Required Uses and Disclosures That May be Made Without Authorization or Opportunity to Object.** Subject to specific terms and conditions addressed in Section 4, DoD covered entities may use or disclose PHI without the individual's authorization or opportunity to object in the following situations:

- (a) When required by law, as provided in Paragraph 4.4.a.
- (b) For public health purposes, as provided in Paragraph 4.4.b.
- (c) Involving victims of abuse or neglect, as provided in Paragraph 4.4.c.
- (d) For health oversight activities authorized by law, as provided in Paragraph 4.4.d.
- (e) For judicial or administrative proceedings, as provided in Paragraph 4.4.e.
- (f) For law enforcement purposes, as provided in Paragraph 4.4.f.
- (g) Concerning decedents in limited circumstances, as provided in Paragraph 4.4.g.
- (h) For cadaveric organ, eye, or tissue donation purposes, as provided in Paragraph 4.4.h.
- (i) For research involving minimal risk, as provided in Paragraph 4.4.i.
- (j) To avert a serious threat to health or safety, as provided in Paragraph 4.4.j.
- (k) For specialized government functions, including certain activities relating to Military Services' personnel, as provided in Paragraph 4.4.k.
- (l) For workers' compensation programs, as provided in Paragraph 4.4.l.

c. Uses and Disclosures of PHI Special Rules and Requirements. A number of special rules and other requirements relating to uses and disclosures of PHI are established. As provided in Paragraph 4.5., these include:

- (1) Standards for de-identification of PHI, as provided in Paragraph 4.5.a.

(2) Requirements for using and disclosing the minimum amount necessary to accomplish a valid use or disclosure purpose, as provided in Paragraph 4.5.b.

(3) Clarification regarding incidental uses and disclosures, as provided in Paragraph 4.5.d.

(4) Disclosures to business associates, as provided in Paragraph 4.5.e.

(5) Disclosures by whistleblowers and workforce member crime victims, as provided in Paragraph 4.5.f.

(6) Rules for dealing with personal representatives on behalf of individuals, as provided in Paragraph 4.5.g.

d. DoD Covered Entity Obligations Regarding Individual Rights. In general, DoD covered entities are obligated to fulfill individual rights stated in the HIPAA Privacy Rule to:

(1) Receive a notice of the ways the MHS may use and disclose their PHI, and of their rights and the MHS' legal duties with respect to PHI, as provided in Paragraph 5.1.

(2) Request additional privacy protections, as provided in Paragraph 5.2. This includes a right to request restrictions on certain uses and disclosures, and a right to receive confidential communications by alternative means or at alternative locations when reasonable, as provided in Paragraphs 5.2.a. and 5.2.b.

(3) Access to inspect and obtain a copy of PHI about them, subject to some limitations, as provided in Paragraph 5.3.

(4) Amend PHI about them if it is inaccurate or incomplete, under procedures outlined in Paragraph 5.4.

(5) Receive, upon request, an accounting of certain disclosures of their PHI, as provided in Paragraph 5.5.

(6) To ensure compliance with the obligations related to the fulfillment of individual rights, DoD covered entities must require that workforce members adhere to the implementation specifications outlined in Section 5 when workforce members seek to exercise their individual rights.

e. Breach Response Provisions. The Final Rule for Breach Notification for Unsecured Protected Health Information, issued by HHS pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, is codified in Parts 160 and 164, Subpart D, of Title 45, CFR (Subpart D is also known as the "HIPAA Breach Rule"). These breach response requirements for the MHS, DoD covered entities, and their business associates are in Section 6.

f. Additional Administrative Requirements for the MHS to Implement Health Information Privacy Protections. To the extent provided in Section 7, the MHS and each DoD

covered entity is required to implement a series of administrative requirements to protect the privacy of health information, including the:

- (1) Designation of a HIPAA privacy officer, as provided in Paragraphs 2.1.c., 2.2.c.(1), and 7.1.a.
- (2) Training of the workforce involved in functions covered by this issuance as provided in Paragraph 7.1.b.
- (3) Establishment of administrative, technical, and physical safeguards to protect the privacy of PHI as provided in Paragraph 7.3.a.
- (4) Creation of a complaint process, as provided in Paragraph 7.2.a.
- (5) Establishment of appropriate policies, procedures, and processes for determining and applying sanctions against workforce members who fail to comply with requirements of this issuance, as provided in Paragraph 7.1.c.
- (6) Mitigation of harmful effects of improper uses and disclosures of PHI, as provided in Paragraph 7.3.b.
- (7) Prohibition of intimidating or retaliatory acts relating to the exercise of rights under this issuance, as provided in Paragraph 7.2.b.
- (8) Prohibition from requiring individuals to waive rights under this issuance, as provided in Paragraph 7.2.c.
- (9) Implementation of policies and procedures to implement privacy protections, as provided in Paragraph 7.3.c.
- (10) Documentation and retention requirements of this issuance, as provided in Paragraph 7.3.d.
- (11) Compliance with transition provisions for individual authorizations effective prior to publication of this issuance are provided in Paragraph 7.4.a.

3.2. SCOPE, ENFORCEMENT, AND RELATIONSHIP TO OTHER LAWS.

a. Inspector General. Pursuant to Section 1320a-7c(a)(5) of Title 42, U.S.C., nothing in this issuance should be construed to diminish the authority of any statutory Inspector General, including such authority as provided in the Appendix of Title 5, U.S.C., also known as the “Inspector General Act of 1978.”

b. Preemption of State Law. Subject to the exceptions specified in this paragraph, this issuance generally applies to the activities of the MHS without regard to contrary provisions of State law. In general, the HIPAA Privacy Rule establishes rules, exceptions, and procedures governing the determination of the preemption of State law.

(1) As a general rule, a standard, requirement, or implementation specification adopted under the HIPAA Privacy Rule that is contrary to a provision of State law preempts the provision of State law. Exceptions include circumstances in which the provision of State law, including State procedures established under such law, as applicable, provide for the reporting of disease or injury, child or domestic abuse or neglect, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(2) State laws pertaining to health care generally are not applicable to DoD health care programs and activities. However, there are some matters in which DoD rules and procedures call for the DoD Components to follow State law.

(a) In cases involving disclosure of PHI about a minor to a parent, guardian, or person acting *in loco parentis* of such minor, the State law where the treatment is provided must be applied.

(b) If there is a conflict between this issuance and State law, this issuance must apply, unless DoD rules, procedures, or other applicable policy call for the DoD Components to follow State law with respect to the matter at issue.

c. Compliance and Enforcement by the Secretary of HHS.

(1) **Applicability of HHS Rules and Procedures to DoD.** Rules and procedures established by the Secretary of HHS pursuant to the HIPAA rules for covered entities and their business associates are applicable through this Manual to DoD covered entities and their business associates.

(2) Complaints to HHS.

(a) **Complaint Submissions.** A person who believes the MHS, a DoD covered entity within the MHS, or a business associate is not complying with the applicable requirements of the HIPAA Privacy, Breach, or Security Rules, may file a complaint with HHS pursuant to Section 160.306 of Title 45, CFR. Such complaints must meet the following requirements established by HHS:

1. A complaint must be filed in writing, either on paper or electronically.
2. A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of the HIPAA rules.
3. A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless the Secretary of HHS waives this time limit for good cause shown.
4. The Secretary of HHS may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register. The HHS complaint form and instructions for filing a complaint are available through the HHS Office for Civil Rights and its website.

(b) HHS Investigation.

1. In Part 160, Subparts C-E, of Title 45, CFR, also known and referred to in this issuance as the “HIPAA Enforcement Rule,” Section 160.306(c)(1) requires the Secretary of HHS to investigate any complaint filed under Section 160.306 of Title 45, CFR, when a preliminary review of the facts indicates a possible violation due to willful neglect.

2. The Secretary of HHS may investigate any other complaint filed under Section 160.306 of Title 45, CFR.

3. Such investigation may include a review of the pertinent policies, procedures, or practices of the MHS (including any supplemental or local policies, procedures, or practices at the DoD covered entity-level) or business associate, and of the circumstances regarding any alleged acts or omissions concerning compliance.

4. At the time of the initial written communication with the MHS, DoD covered entity, or business associate about the complaint, the Secretary of HHS will describe the acts or omissions that are the basis of the complaint, as required by Section 160.306(c)(4) of the HIPAA Enforcement Rule.

(3) Compliance Reviews.

(a) Section 160.308(a) of Title 45, CFR requires the Secretary of HHS to conduct compliance reviews to determine whether a covered entity or business associate is complying with the applicable requirements of the HIPAA rules when a preliminary review of the facts indicates a possible violation due to willful neglect.

(b) The Secretary of HHS may conduct a compliance review to determine whether a covered entity or business associate is complying with the HIPAA rules in any other circumstance.

(4) Responsibilities of Covered Entities in Relation to HHS Compliance and Enforcement.

(a) **Records and Compliance Reports.** A covered entity or business associate must keep records and submit compliance reports, in such time and manner and containing such information as the Secretary of HHS determines necessary, to ascertain whether the covered entity or business associate has complied or is complying with the applicable requirements of the HIPAA rules.

(b) **Cooperate With Complaint Investigations and Compliance Reviews.** A covered entity or business associate must cooperate with the Secretary of HHS if the Secretary of HHS undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity or business associate to determine whether it is complying with the HIPAA rules.

(c) Permit Access to Information.

1. A covered entity or business associate must permit the Secretary of HHS access during normal business hours to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the applicable requirements of the HIPAA rules. If the Secretary of HHS determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary of HHS at any time and without notice.

2. If any information required of a covered entity or business associate under this paragraph is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.

3. PHI obtained by the Secretary of HHS in connection with an investigation or compliance review will not be disclosed by the Secretary of HHS, except if necessary for ascertaining or enforcing compliance with the applicable requirements of the HIPAA rules, or if otherwise required by law.

4. In the event any information sought by the Secretary of HHS under Paragraph 3.2.c.(4)(c) is classified in the interest of national security or defense, the covered entity or business associate must make appropriate arrangements for access by the Secretary of HHS consistent with applicable requirements for handling classified information.

(5) **Penalties for Non-compliance.** Section 1320d-6 of Title 42, U.S.C., establishes civil and criminal penalties for non-compliance with the HIPAA rules. For HIPAA Rule violations occurring on or after February 18, 2009, there are:

(a) Civil penalties of not less than \$100 for each violation.

(b) Civil penalties of not more than \$1,500,000 when identical violations during a calendar year occur.

(c) Criminal penalties of fines of up to \$250,000 and imprisonment up to 1 year, for wrongful disclosure by any covered entity, employee, or other individual of individually identifiable health information.

(6) **Violations Attributed to Covered Entity.** The covered entity is liable, in accordance with the federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

(7) **Privacy Violations of Business Associates.** A business associate is liable, in accordance with the federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or a subcontractor, acting within the scope of the agency.

d. Relationship to the Privacy Act. In addition to responsibilities for compliance with this issuance, DoD covered entities are also responsible for compliance with DoD Privacy Program issuances.

(1) Although nothing in this issuance violates DoD Privacy Program issuances, compliance with this issuance does not necessarily satisfy all the requirements of the DoD Privacy Program issuances. For example, an authorized disclosure under Paragraph 4.4. may require additional actions, such as the establishment of a “routine use” in the system of records notice for the system of records in which the PHI is maintained, which specifically identifies to whom the disclosure is made and for what purpose.

(2) Compliance with the DoD Privacy Program issuances in connection with PHI does not necessarily satisfy all the requirements of this issuance. For example, an authorized routine use of medical records under the DoD Privacy Program issuances is not necessarily a permitted use or disclosure under this issuance.

(3) Nothing in this issuance creates an individual right or DoD obligation under the DoD Privacy Program issuances (i.e., DoDD 5400.11 or DoD 5400.11-R).

e. No Private Cause of Action.

(1) There is no private cause of action under the HIPAA rules or this issuance. Potential remedies for alleged violations of the HIPAA rules are those referred to in Paragraph 3.2.c. Potential remedies for alleged violations of this issuance are addressed in Paragraphs 7.1.c. and 7.2.a. Nothing in this issuance gives an individual a right to initiate a legal action in court for any alleged violations.

(2) Although, as stated in Paragraph 3.2.d., there is overlap between this issuance and DoD Privacy Program issuances, alleged or actual violations of this issuance do not necessarily constitute a violation of DoD Privacy Program issuances or give rise to a cause of action under the Privacy Act.

f. Relationship to Section 552 of Title 5, U.S.C., Also Known as the “Freedom of Information Act (FOIA).”

(1) In general, FOIA requires federal agencies to make available the records in the possession of the agencies to members of the public who request them. FOIA, however, is subject to exemptions, such as when such disclosure would cause an unwarranted invasion of the personal privacy of an individual or privacy of other individuals such as a deceased individual’s surviving family members.

(2) Access to PHI, other than that specifically provided for in this issuance, would generally cause an unwarranted invasion of personal privacy of the individual to whom the PHI pertains. However, in any case in which FOIA requires disclosure, nothing in this Manual prohibits disclosure.

(3) Requests under FOIA are handled in accordance with DoDM 5400.07. Application of FOIA exemptions to information about deceased individuals requires a different analysis than that applicable to living individuals and is provided in Paragraph 4.5.h.

3.3. ORGANIZATIONAL ROLES AND RESPONSIBILITIES. DoD covered entities, and DoD Components that are business associates of DoD covered entities, must take on certain roles and responsibilities to comply with this issuance.

a. Covered Entities in the MHS.

(1) The MHS is comprised of the following DoD covered entities: all DoD health plans and all DoD institutional health care providers that engage in standard electronic transactions and that are organized under the management authority of, or individual providers assigned to or employed by, any of the following:

- (a) DHA.
- (b) The Department of the Army.
- (c) The Department of the Navy.
- (d) The Department of the Air Force.

(2) Not all health care providers affiliated with the Military Services are DoD covered entities. DoD health care provider covered entities include:

(a) Health care personnel and related assets of the Department of the Army under the Surgeon General of the Army, including Headquarters staff, including any other organizational level within the Army Medical Service, and the DoD covered entity identified in Paragraph 3.3.a.(4)(b)1. Policies and procedures supplementing MHS-wide HIPAA policies are principally established by the Surgeon General of the Army, but may also be established by or on behalf of the Chief of Staff of the Army, the Assistant Secretary of the Army for Manpower and Reserve Affairs, or the Secretary of the Army.

(b) Health care personnel and related assets of the Department of the Navy under the Surgeon General of the Navy, including any other organizational level within the Navy, and the DoD covered entity identified in Paragraph 3.3.a.(4)(b)2. Policies and procedures supplementing MHS-wide HIPAA policies are principally established for Navy health care personnel and related assets by the Surgeon General of the Navy, but may also be established by or on behalf of the Chief of Naval Operations, the Assistant Secretary of the Navy for Manpower and Reserve Affairs, or the Secretary of the Navy.

(c) Health care personnel and related assets of the Department of the Air Force under the Surgeon General of the Air Force and the DoD covered entity identified in Paragraph 3.3.a.(4)(b)3. Policies and procedures supplementing MHS-wide HIPAA policies are principally established for Air Force health care personnel and related assets by the Surgeon General of the Air Force, but may also be established by or on behalf of the Chief of Staff of the

Air Force, the Assistant Secretary of the Air Force for Manpower and Reserve Affairs, or the Secretary of the Air Force.

(d) Health care personnel and related assets of the DHA, including the MTFs that operate under the authority of the DHA. Policies and procedures supplementing MHS-wide HIPAA policies are principally established for DHA health care personnel and related assets by the Director, DHA, or the Director's designee.

(3) All such covered entities are under the common control of the ASD(HA). These DoD covered entities are designated as a single HIPAA covered entity under the management control of the ASD(HA), and, for purposes of activities subject to this issuance, under the management responsibility of the Director, DHA.

(4) In carrying out responsibilities in this issuance, including appointment of HIPAA privacy and security officers, each DoD covered entity (such as an MTF) must establish its own supplementary policies and procedures for complying with this issuance and directions of the Director, DHA.

(a) Contracted health care providers providing personal services or non-personal services to the MTF, are required to comply with all requirements of or arising from this issuance to the same extent as health care providers who are employees of the MTF. It is the responsibility of the DoD component that establishes the contract to ensure that it includes requirements under this Manual.

(b) All health care providers who are DoD covered entities under this issuance and who are not providing services in or on behalf of an MTF (for example, shipboard or field deployed medical personnel) are included in a DoD covered entity, as follows:

1. Providers under the control of the Department of the Army are included in a DoD covered entity under the Surgeon General of the Army.

2. Providers under the control of the Department of the Navy are included in a DoD covered entity under the Surgeon General of the Navy.

3. Providers under the control of the Department of the Air Force are included in a DoD covered entity under the Surgeon General of the Air Force.

(5) Policies and procedures for the MHS are established principally by the ASD(HA) as authorized by DoDD 5136.01, but may also be established by the Under Secretary of Defense for Personnel and Readiness or the Secretary of Defense. Such policies and procedures may also be established by the Director, DHA, to the extent of the Director's authorities in accordance with DoDD 5136.13, or as otherwise delegated by the ASD(HA).

b. The MHS and Organized Health Care Arrangements.

(1) For certain purposes under this issuance, such as the establishment of a DoD covered entity's rules and procedures for uses and disclosures of PHI for treatment, payment, or health care operations, such rules and procedures established by an organized health care arrangement

of which the DoD covered entity is a part are recognized as the rules and procedures of the DoD covered entity. For this purpose, the MHS, as a single covered entity, and certain elements of the Coast Guard are identified as an organized health care arrangement.

(2) The MHS is also part of an organized health care arrangement with the Coast Guard. The following elements of the Coast Guard are part of that organized health care arrangement:

(a) Providers under the control of the Commandant, U.S. Coast Guard; and under the Director, Health, Safety, and Work-life Directorate of the U.S. Coast Guard.

(b) The Coast Guard Health Care Program.

c. Business Associate Arrangements among and for DoD Components.

(1) **Arrangements for Government and Non-Government Business Associates.** DoD Components sometimes perform functions for covered entities that are covered functions under this issuance. In other cases, business associate functions for DoD covered entities may be carried out by other government agencies or by non-governmental entities under contract. Business associates are:

(a) DoD Components that do not require a written business associate agreement.

(b) Other government agencies that require a memorandum of agreement (or other applicable documentation of the arrangement) between the DoD Component and the other government agency.

(c) Other entities that require a contract or agreement between the DoD Component and the other entity, in accordance with Paragraphs 3.3.c.(2) and 4.5.e.(3).

(2) Business Associate Contracts.

(a) The contract or other arrangement required by Paragraph 4.5.e.(3) must establish the permitted and required uses and disclosures of PHI by the business associate, and must also meet the requirements of Paragraphs 3.3.c.(1)(b) and (c), 3.3.c.(3), or 3.3.c.(5), as applicable.

(b) A DoD covered entity is not in compliance with the standards in Paragraph 4.5.e.(3) and this paragraph if the DoD covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the DoD covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(c) A business associate is not in compliance with the standards in Paragraph 4.5.e.(2) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(3) **Business Associate Uses and Disclosures.** DHA guidance provides standard business associate agreement language to be included, when appropriate, in contracts or agreements that involve access to or handling of PHI by DoD covered entity business associates. The DHA standard language is designed to satisfy the following requirements applicable to uses and disclosures of PHI by business associates. Additional requirements may be included in contracts and agreements at the discretion of the DoD covered entity.

(a) A business associate may not use or further disclose PHI in a manner that would violate the requirements of this issuance if done by the DoD covered entity, except that the business associate may engage in the following uses and disclosures if permitted by its contract or other arrangement:

1. A business associate may use and disclose PHI for the proper management and administration of the business associate.

2. A business associate may provide data aggregation services relating to the health care operations of the DoD covered entity.

(b) A business associate must:

1. Use or disclose PHI only as permitted or required by this issuance or as required by law.

2. Use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule and other DoD cybersecurity requirements with respect to electronic PHI, to prevent use or disclosure of the information other than as allowed by this issuance.

3. Report to the DoD covered entity any use or disclosure of PHI not allowed by this issuance (or by the contract with the DoD covered entity) of which the business associate becomes aware. This includes breaches as required by Section 6.

4. Ensure any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such PHI in accordance with the HIPAA Privacy Rule.

5. Make available PHI in accordance with the access provisions of Paragraph 5.3., including Paragraph 5.3.c.(2)(a) regarding access to information and Paragraph 5.3.c.(2)(d) regarding individual directions to transmit information to a person designated by the individual.

6. Make available PHI for amendment and incorporate any amendments to PHI in accordance with Paragraph 5.4.

7. Make available the information required to provide an accounting of disclosures in accordance with Paragraph 5.5.

8. To the extent the business associate is to carry out a DoD covered entity's obligations under this issuance, comply with the requirements of this issuance that apply to the DoD covered entity in the performance of such obligation.

9. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the DoD covered entity available to the Secretary of HHS and to the Director, DHA, for purposes of investigating or determining the DoD covered entity's compliance with the HIPAA rules.

10. Return or destroy, at the termination of the performance of the business associate's functions, all PHI received from, or created or received by the business associate on behalf of the DoD covered entity that the business associate still maintains in any form. If such return or destruction is not feasible, the business associate must maintain compliance with this issuance with respect to any retained copies of the information, and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. Any action taken should be appropriately documented.

(4) Other Arrangements.

(a) If a DoD covered entity and its business associate are both government entities:

1. The DoD covered entity may comply with this paragraph and Enclosure 4, Paragraph 1.i.(5) of DoDI 8580.02, if applicable, by entering into a memorandum of understanding with the business associate that contains the terms that accomplish the objectives of Paragraph 3.3.c.(3) and Enclosure 4, Paragraph 1.i.(5)(a) of DoDI 8580.02, if applicable.

2. The DoD covered entity may comply with this paragraph and Enclosure 4, Paragraph 1.i.(5) of DoDI 8580.02, if applicable, if other law (including regulations adopted by the DoD covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of Paragraph 3.3.c.(3) and Enclosure 4, Paragraph 1.i.(5)(a) of DoDI 8580.02, if applicable.

(b) If a business associate is required by law to perform a function or activity on behalf of a DoD covered entity or to provide a service described in the definition of business associate in this issuance to a DoD covered entity, such DoD covered entity may disclose PHI to the business associate necessary to comply with the legal mandate. This may be done without meeting the requirements of Paragraph 3.3.c. and Enclosure 4, Paragraph 1.i.(5) of DoDI 8580.02, if applicable, if the DoD covered entity attempts in good faith to obtain satisfactory assurances that the business associate will honor the provisions of Paragraph 3.3.c.(3)(b) and Enclosure 4, Paragraph 1.i.(5) of DoDI 8580.02, if applicable. If such attempt fails, the attempt and the reasons that such assurances cannot be obtained must be documented.

(c) The DoD covered entity may comply with this paragraph and Enclosure 4, Paragraph 1.i.(5) of DoDI 8580.02, if the DoD covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the DoD covered entity has a data use agreement with the business associate that complies with Paragraph 4.5.c.(4)(a) and Enclosure 4, Paragraph 1.i.(5) of DoDI 8580.02, if applicable.

(5) Other Requirements for Contracts and Other Arrangements.

(a) The contract or other arrangement may allow the business associate to use PHI:

1. For the proper management and administration of the business associate.
2. To carry out the legal responsibilities of the business associate.

(b) The business associate may disclose PHI for the purposes described in Paragraph 3.3.c.(5)(a), if:

1. The disclosure is required by law; or
2. The business associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which the disclosure was intended and the person notifies the business associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

(6) **Applicability to subcontractors.** The requirements of Paragraphs 3.3.c.(3) and 3.3.c.(4) apply to the contract or other arrangement required by the HIPAA Privacy Rule between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a DoD covered entity and business associate.

d. Requirements for a Covered Entity with Multiple Covered Functions.

(1) A DoD covered entity that performs multiple covered functions that would make the entity a combination of a health plan and a covered health care provider must comply with the standards, requirements, and implementation specifications of this issuance, as applicable to the health plan or health care provider covered functions performed.

(2) A DoD covered entity that performs multiple covered functions may use or disclose the PHI of individuals who receive the DoD covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

e. DoD as a Hybrid Entity. Not all components within the DoD carry out covered functions. DoD Components that solely provide non-covered functions and do not act as business associates are not subject to the requirements of this issuance. Only DoD covered entities within the MHS and DoD Components that are business associates to the MHS must comply with the requirements of this issuance.

SECTION 4. USES AND DISCLOSURES OF PHI

4.1. GENERAL RULES ON USES OR DISCLOSURES OF PHI.

a. Standard: Permitted and Prohibited Uses and Disclosures.

(1) **Permitted Uses and Disclosures.** Except for uses or disclosures that require an authorization under Paragraphs 4.2.a.(2), 4.2.a.(3), and 4.2.a.(4) or that are prohibited under Paragraph 4.5.k., a DoD covered entity may use or disclose PHI for treatment, payment, or health care operations described in Paragraph 4.1.b., provided that such use or disclosure is consistent with other applicable requirements of this issuance.

(2) **Prohibited Uses and Disclosures.** Notwithstanding any other provision of this issuance, a DoD covered entity must not use or disclose PHI for which:

(a) The Privacy Act would prohibit the use or disclosure absent written consent from the individual to whom the information relates, as provided in Paragraph 5.3.a.(4).

(b) The special rules for substance use disorder program patient records would prohibit the use or disclosure absent a specific written consent from the individual to whom the information relates, as provided in Paragraph 4.5.j.

(c) The special rules for genetic information would prohibit the use or disclosure for health plan underwriting purposes, as provided in Paragraph 4.5.k.

(d) Paragraph 4.2.a.(4) would prohibit the use or disclosure through a sale absent compliance with the requirements of Paragraph 4.2.a.(4).

b. Implementation Specifications: Treatment, Payment, and Health Care Operations. A DoD covered entity may:

(1) Use or disclose PHI for its own treatment, payment, or health care operations.

(2) Disclose PHI for treatment activities of a health care provider.

(3) Disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) Disclose PHI to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is for:

(a) A purpose listed in the definition of health care operations; or

(b) The purpose of health care fraud and abuse detection or compliance.

(5) If participating in an organized health care arrangement, may disclose PHI about an individual to another DoD covered entity that participates in the organized health care arrangement for any health care operations activities of the arrangement.

c. Implementation Specifications: Disclosures through Health Information Exchange.

This paragraph applies to permissible uses and disclosures made through health information exchange arrangements such as the eHealth Exchange and the Virtual Lifetime Electronic Record Health Information Exchange with respect to health care beneficiaries who are not members of the Uniformed Services (referred to in this paragraph as “MHS non-active duty health care recipients”) but who are identified as eligible for MHS health benefits in the Defense Manpower Data Center Defense Enrollment and Eligibility Reporting System and whose data are available in the MHS Central Data Repository.

(1) MHS non-active duty health care recipients’ data are available for sharing through all health information exchange arrangements in which the MHS participates.

(2) MHS non-active duty health care recipients must be given an opportunity to, at any time, opt out of sharing their health information with non-MHS organizations.

(3) MHS non-active duty health care recipients must be given an opportunity to revoke a prior opt out election by choosing to opt back in.

4.2. USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION IS REQUIRED.

a. Standard Operating Procedures. Each DoD covered entity must establish standard operating procedures for uses and disclosures of PHI which require an authorization as covered in this paragraph.

(1) **General Rule.** Except as otherwise permitted or required by this issuance, a DoD covered entity may not use or disclose PHI without an authorization that is valid under Paragraph 4.2. When a DoD covered entity obtains or receives a valid authorization for use or disclosure of PHI, any use or disclosure must be consistent with such authorization. An authorization is ineffective and does not permit a DoD covered entity or business associate to use or disclose genetic information if the use or disclosure is prohibited by Paragraph 4.5.k.

(2) **Psychotherapy Notes.** Notwithstanding any other provision of this issuance, other than transition provisions provided for in Paragraph 7.4., a DoD covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(a) To carry out the following treatment, payment, or health care operations:

1. Use by the originator of the psychotherapy notes for treatment.

2. Use or disclosure by the DoD covered entity for its own training programs through which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling.

3. Use or disclosure by the DoD covered entity to defend itself in a legal action or other proceeding brought by the individual whose PHI is used or disclosed. Uses or disclosures permitted under this paragraph include those to defend the United States in a claim or action brought pursuant to Sections 2671-2680, Title 28, U.S.C., also known as the Federal Tort Claims Act, or Chapter 163 of Title 10, U.S.C., also known as the Military Claims Act, and arising from any alleged act or omission of the DoD covered entity.

(b) A use or disclosure that is:

1. Required by the Secretary of HHS in relation to compliance activities of the Secretary of HHS referred to in Paragraph 3.2.c.

2. Permitted by Paragraph 4.4.a., pertaining to uses and disclosures required by law.

3. Permitted by Paragraph 4.4.d., pertaining to uses and disclosures for health oversight activities with respect to the originator of psychotherapy notes.

4. Permitted by Paragraph 4.4.g., pertaining to uses and disclosures about decedents to coroners and medical examiners.

5. Permitted by Paragraph 4.4.j.(1)(a), pertaining to uses and disclosures to avert a serious and imminent threat to the health or safety of a person or the public, which may include a serious and imminent threat to military personnel or members of the public, or a serious imminent threat to a specific military mission or national security under circumstances that in turn create a serious and imminent threat to a person or the public.

(3) Authorization Required: Marketing.

(a) Notwithstanding any provision of this issuance, other than the transition provisions in Paragraph 7.4., a DoD covered entity must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

1. A face-to-face communication made by a DoD covered entity to an individual;
or

2. A promotional gift of nominal value provided by the DoD covered entity.

(b) If the marketing involves payment to the DoD covered entity from a third party, the authorization must state that such payment is involved.

(4) Authorization Required: Sale. Notwithstanding any provision of this issuance, a DoD covered entity may not sell an individual's PHI unless:

(a) The DHA Privacy Office has determined, in writing, that such sale is permitted by applicable DoD issuances or other applicable publications.

(b) The covered entity has obtained an authorization from each individual whose PHI is subject to such sale.

b. Implementation Specifications: General Requirements.

(1) Valid Authorizations.

(a) A valid authorization must contain the elements listed in Paragraphs 4.2.b.(3)(a), 4.2.c.(1), and 4.2.c.(2), as applicable.

(b) A valid authorization may contain elements or information in addition to the elements required by Paragraph 4.2., provided that such additional elements or information are not inconsistent with the elements required by Paragraph 4.2.

(2) Defective Authorizations. An authorization is not valid if the document submitted has any of the following defects:

(a) The expiration date has passed or the expiration event is known by the DoD covered entity to have occurred.

(b) The authorization has not been filled out completely with respect to an element described by Paragraph 4.2.c., if applicable.

(c) The authorization is known by the DoD covered entity to have been revoked.

(d) The authorization violates Paragraphs 4.2.b.(3) or 4.2.b.(4), if applicable.

(e) Any material information in the authorization is known by the DoD covered entity to be false.

(3) Compound Authorizations. An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except:

(a) An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research.

1. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under Paragraph 4.2.b.(4), any compound authorization created under Paragraph 4.2. must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

2. If an authorization includes both conditioned and unconditioned components of the research activity, each conditioned and unconditioned component of the research activity in the authorization must be signed separately by the individual or the individual's personal representative.

(b) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(c) An authorization under Paragraph 4.2., other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under Paragraph 4.2., except when a DoD covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under Paragraph 4.2.b.(4) on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under Paragraph 4.2.b.(4) of this issuance does not apply to a compound authorization created in accordance with Paragraph 4.2.b.(3)(a)1.

(4) **Prohibition on Conditioning of Authorizations.** A DoD covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(a) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research under Paragraph 4.2.

(b) A DoD covered entity may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party. Examples of this include physical exams performed in order for a family member to participate in a school's extracurricular activities.

(5) **Revocation of Authorizations.** An individual may revoke an authorization provided under this Paragraph 4.2. at any time, provided the revocation is in writing, except to the extent that either Paragraphs 4.2.b.(5)(a) or 4.2.b.(5)(b) applies. Paragraph 4.2.b.(5)(c) governs revocation of a compound authorization involving a research study.

(a) The DoD covered entity has taken action in reliance thereon; or

(b) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(c) Where an individual has revoked a compound authorization involving research studies (see Paragraph 4.2.b.(3)(a)), the entire authorization must be treated as revoked, unless such revocation is clear about what research activities to which the revocation applies and does not apply. Where the scope of the revocation is not clear, written clarification must be obtained from the individual.

(6) **Documentation.** A DoD covered entity must document and retain any signed authorization or revocation as required by Paragraph 7.3.d.

(7) **Review of Authorizations.** A DoD covered entity must review on a periodic basis any authorization provided under Paragraph 4.2. If the review discloses any question over the authorization's continuing validity, the DoD covered entity must contact the individual who provided the authorization to clarify and, if necessary, verify contents of the authorization.

(8) **Processing of Authorizations.** Authorizations involving use or disclosure of PHI in the possession of a DoD covered entity must be directed to the HIPAA privacy officer for that DoD covered entity.

c. Implementation Specifications: Core Elements and Requirements.

(1) **Core Elements.** A valid authorization under Paragraph 4.2. must contain at least the following elements:

(a) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(b) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(c) The name or other specific identification of the person(s), or class of persons, to whom the DoD covered entity may make the requested use or disclosure.

(d) A description of each purpose of the requested use or disclosure.

1. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

2. In the case of an authorization for research purposes, the stated purpose need not be specific to a current research study.

3. An authorization for future studies is permissible, provided that the future research purposes are adequately described such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future studies. The purposes of such future studies may be described in a more general manner than is done for specific current studies, provided that research of unusual sensitivity should be described if such research is contemplated at the time of the authorization.

(e) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for the use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository.

(f) Signature of the individual and the date the individual signed. If a personal representative of the individual signs the authorization, a description of such representative's authority to act for the individual must also be provided.

(2) **Required Statements.** In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of:

(a) The individual's right to revoke the authorization in writing, and either:

1. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

2. A reference to the DoD covered entity's notice, to the extent that the information in Paragraph 4.2.c.(2)(a)1. is included in the notice required by Paragraph 5.1.

(b) The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating either:

1. The DoD covered entity may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in Paragraph 4.2.b.(4) applies;

2. The consequences to the individual of a refusal to sign the authorization when, in accordance with Paragraph 4.2.b.(4), the DoD covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization; or

3. The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and to no longer be protected by this issuance or the HIPAA Privacy Rule.

(3) **Plain Language Requirement.** The authorization must be written in plain language. Guidance on plain language is available on the DoD Directives Division Website, in accordance with DoDI 5025.13, and Public Law 111-274, known as the "Plain Writing Act of 2010."

(4) **Copy to the Individual.** If a DoD covered entity seeks an authorization from an individual for a use or disclosure of PHI, the DoD covered entity must provide the individual with a copy of the signed authorization.

(5) **DD Form 2870.** Individual authorization for use or disclosure of PHI may be documented on DD Form 2870, "Authorization for Disclosure of Medical or Dental Information." A copy of the form is available on the DHA Privacy Office website.

4.3. USES AND DISCLOSURES REQUIRING AN OPPORTUNITY FOR INDIVIDUAL TO AGREE OR TO OBJECT. A DoD covered entity may use or disclose PHI when the individual is informed in advance of the use or disclosure and has the opportunity to agree to, prohibit, or restrict the disclosure, in accordance with the applicable requirements of this paragraph. The DoD covered entity may orally inform the individual of, and obtain the

individual's oral agreement or objection to, a use or disclosure permitted by this issuance. If an individual objects, that objection must be documented by the DoD covered entity and must remain valid for the duration of that episode of care.

a. Standard: Use and Disclosure for Facility Directories.

(1) **Permitted Uses and Disclosure.** Except when an objection is expressed in accordance with Paragraphs 4.3.a.(2) or 4.3.a.(3), a covered health care provider may:

(a) Use the following PHI to maintain a directory of individuals in its facility:

1. The individual's name.
2. The individual's location in the covered health care provider's facility.
3. The individual's condition described in general terms, that does not communicate specific medical information about the individual, such as "stable," "good," "fair," "serious," "critical," "conscious," "semiconscious," and "unconscious."
4. The individual's religious affiliation for use by members of the clergy.

(b) Use PHI for directory purposes or disclose for same purposes to:

1. Members of the clergy.
2. Except for religious affiliation, to other persons who ask for the individual by name.

(2) **Opportunity to Object.** A covered health care provider must give an individual the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by Paragraph 4.3.a.(1). If an individual objects, that objection must be documented by the DoD covered entity and will remain valid for the duration of that episode of care.

(3) **Emergency Circumstances.**

(a) A covered health care provider may use or disclose some or all of an individual's PHI when an individual is incapacitated or emergency treatment is required. Disclosure of PHI is permitted by Paragraph 4.3.a.(1) for the facility's directory, if such disclosure is:

1. Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider.
2. In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(b) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by Paragraph 4.3.a.(2) when it becomes practicable to do so.

b. Standard: Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes.

(1) Permitted Uses and Disclosures.

(a) A DoD covered entity may, in accordance with Paragraph 4.3.b.(2), 4.3.b.(3), or 4.3.b.(5) disclose to a family member, other relative, close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(b) A DoD covered entity may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes must be in accordance with Paragraph 4.3.b.(2), 4.3.b.(3), 4.3.b.(4), or 4.3.b.(5), as applicable.

(2) **Uses and Disclosures with the Individual Present.** If the individual is present for, or otherwise available prior to, a use or disclosure permitted by Paragraph 4.3.b.(1) and has the capacity to make health care decisions, the DoD covered entity may use or disclose the PHI if it:

(a) Obtains the individual's agreement;

(b) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(c) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) **Limited Uses and Disclosures When the Individual Is Not Present.**

(a) If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the DoD covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes.

(b) A DoD covered entity may use professional judgment and its experience with common practice and guidance from respective Service regulations to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

(4) **Use and Disclosures for Disaster Relief Purposes.** A DoD covered entity may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by Paragraph 4.3.b.(1)(b). The requirements in Paragraphs 4.3.b.(2), 4.3.b.(3), and 4.3.b.(5) apply to such uses and disclosures to the extent that the DoD covered entity, in the exercise of

professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) Uses and Disclosures When the Individual Is Deceased.

(a) A DoD covered entity may disclose a deceased individual's PHI to a family member or other person identified in Paragraph 4.3.b.(1)(a) if such family member or person was involved in the care or payment for health care of the individual before the individual's death. A permitted disclosure of the deceased individual's PHI under the preceding sentence is subject to the following limitations:

1. The disclosed PHI must be relevant to the person's involvement with the deceased individual.
2. Disclosure of the PHI does not conflict with any prior expressed preferences of the deceased individual known to the DoD covered entity.

(b) A DoD covered entity may accept a request for disclosure of a deceased individual's PHI as a request submitted to DoD through FOIA, and act upon such request in accordance with both FOIA and the HIPAA Privacy Rule.

4.4. USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED. A DoD covered entity may use or disclose PHI without the written authorization of the individual as described in Paragraph 4.2. or the opportunity for the individual to agree or object as described in Paragraph 4.3., in situations covered by this paragraph, subject to the applicable requirements of this paragraph and its subparagraphs. When the DoD covered entity is required by this paragraph to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this paragraph, the DoD covered entity's information and the individual's agreement may be given orally. In such cases, the DoD covered entity must establish appropriate documentation of such oral communication. As required by Paragraph 3.2.d., a disclosure permitted by this paragraph and its subparagraphs must also be considered under the standards of the Privacy Act and DoD Privacy Program issuances to determine whether the disclosure is also covered and permitted by such standards.

a. Standard: Uses and Disclosures Required by Law.

(1) A DoD covered entity may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A DoD covered entity must meet the requirements described in Paragraphs 4.4.c., 4.4.e., or 4.4.f. for uses or disclosures required by law.

b. Standard: Uses and Disclosures for Public Health Activities.

(1) **Permitted Uses and Disclosures.** A DoD covered entity may use or disclose PHI for public health activities to:

(a) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.

(b) A public health authority or other government authority authorized by law to receive reports of child abuse or neglect.

(c) A person subject to the jurisdiction of the Food and Drug Administration (FDA) addressing an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity. Such purposes include:

1. Collecting or reporting adverse events or similar reports with respect to food or dietary supplements, product defects or problems, including problems with the use or labeling of a product, or biological product deviations.

2. Tracking FDA-regulated products.

3. Enabling product recalls, repairs, replacement, or lookback, including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback.

4. Conducting post-marketing surveillance.

(d) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the DoD covered entity or public health authority is authorized or required by law to notify such person as necessary in the conduct of a public health intervention or investigation.

(e) An employer, about an individual who is a member of the workforce of the employer, if:

1. The DoD covered entity is a health care provider who provides health care to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury.

2. The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance.

3. The employer needs such findings in order to comply with its obligations in accordance with Parts 1904 through 1928 of Title 29, CFR, also known as the “Occupational Safety and Health Administration Regulations;” Parts 50 through 90 of Title 30, CFR, also known as the “Mine Safety and Health Administration Regulations;” or under State law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance.

4. The covered health care provider provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time the health care is provided, or, if the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(f) A school, about an individual who is a student or prospective student of the school, if:

1. The PHI that is disclosed is limited to proof of immunization.

2. The school is required by State or other law to have such proof of immunization prior to admitting the individual.

3. The DoD covered entity obtains and documents the agreement to the disclosure from either:

a. A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

b. The individual, if the individual is an adult or emancipated minor.

(2) **Permitted Uses.** If the DoD covered entity is also a public health authority, the DoD covered entity is permitted to use PHI in all cases for which it is permitted to disclose such information for public health activities under Paragraph 4.4.b.(1).

(3) **DoD Administered Public Health Activities.** Activities of the DoD authorized by applicable DoD issuances or other applicable publications to carry out functions identified in Paragraph 4.4.b.(1) are included as public health activities for purposes of that paragraph.

c. Standard: Disclosures About Victims of Abuse, Neglect, or Domestic Violence.

(1) **Permitted Disclosures.** In addition to the authorities identified in Paragraph 4.4.b.(1)(b), a DoD covered entity may disclose PHI about an individual whom the DoD covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(a) When the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(b) If the individual agrees to the disclosure; or

(c) When the disclosure is expressly authorized by statute or regulation, and

1. The DoD covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

2. If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) Informing the Individual. A DoD covered entity that makes a disclosure permitted by Paragraph 4.4.c.(1) must promptly inform the individual that such a report has been or will be made, except if:

(a) The DoD covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(b) The DoD covered entity would inform the individual's personal representative, but the DoD covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the DoD covered entity, in the exercise of professional judgment.

(3) DoD Domestic Abuse Prevention Activities. Activities of the DoD authorized by applicable DoD issuances or other applicable publications to receive reports of abuse, neglect, or domestic violence consistent with the purpose of Paragraph 4.4.c.(1) are included as authorized government authorities for purposes of that paragraph.

d. Standard: Uses and Disclosures for Health Oversight Activities.

(1) Permitted Disclosures. A DoD covered entity may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(a) The health care system.

(b) Government benefits programs for which health information is relevant to beneficiary eligibility.

(c) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards.

(d) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) **Exception to Health Oversight Activities.** For the purpose of the disclosures permitted by Paragraph 4.4.d.(1), a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

- (a) The receipt of health care.
- (b) A claim for public benefits related to health.
- (c) Qualification for, or receipt of, public benefits or services when an individual's health is integral to the claim for public benefits or services.

(3) **Joint Activities or Investigations.** Notwithstanding Paragraph 4.4.d.(2), if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of Paragraph 4.4.d.

(4) **Permitted Uses.** If a DoD covered entity is also a health oversight agency, the DoD covered entity may use PHI for health oversight activities as permitted by Paragraph 4.4.d.

(5) **DoD Health Oversight Activities.**

(a) Any activity of the DoD authorized by applicable DoD issuances or other applicable publications to carry out health oversight functions is included as a health oversight agency for purposes of Paragraph 4.4.d.

(b) Under the provisions of Executive Order 13181, PHI concerning an individual discovered during the course of health oversight activities will not be used against that individual in an unrelated civil, administrative, or criminal investigation of a non-health oversight matter, unless the General Counsel of the Department of Defense (GC DoD) has authorized such use.

1. DoD health oversight activities will seek and obtain approval for such uses from the GC DoD before such use is made.

2. In assessing whether PHI should be used under Paragraph 4.4.d.(5)(b), the GC DoD will permit such use upon concluding that the balance of relevant factors weighs clearly in favor of its use (i.e., the GC DoD will permit disclosure if the public interest and the need for disclosure clearly outweigh the potential for injury to the individual, to the physician-patient relationship, and to the treatment services).

3. Upon the decision to use PHI under Paragraph 4.4.d.(5)(b), the GC DoD, in determining the extent to which this information should be used, will impose appropriate safeguards against unauthorized use.

4. On an annual basis, the GC DoD will provide the Department of Justice a report that includes the following information:

a. The number of requests made to the GC DoD for authorization to use PHI discovered during health oversight activities in a non-health oversight, unrelated investigation.

b. The number of requests that were granted as applied for, granted as modified, or denied.

c. The DoD Components that made the applications and the number of requests made by each DoD Component.

d. The uses for which the PHI was authorized.

e. Standard: Uses and Disclosures for Judicial and Administrative Proceedings.

(1) **Permitted Disclosures.** A DoD covered entity may disclose PHI in the course of any judicial or administrative proceeding:

(a) In response to an order of a court or administrative tribunal, provided that the DoD covered entity discloses only the PHI expressly authorized by such order.

(b) In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if:

1. The DoD covered entity receives satisfactory assurance, as described in Paragraph 4.4.e.(1)(c), from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the requested PHI has been given notice of the request; or

2. The DoD covered entity receives satisfactory assurance, as described in Paragraph 4.4.e.(1)(d), from the party seeking the information that reasonable efforts were made by such party to secure a qualified protective order that meets the requirements of Paragraph 4.4.e.(1)(e).

(c) For the purposes of Paragraph 4.4.e.(1)(b)1., a DoD covered entity receives satisfactory assurances from a party seeking PHI if the DoD covered entity receives from such party a written statement and accompanying documentation demonstrating that:

1. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address).

2. The notice included sufficient information about the litigation or proceeding for which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal.

3. The time for the individual to raise objections to the court or administrative tribunal has elapsed.

a. No objections were filed; or

b. All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(d) For the purposes of Paragraph 4.4.e.(1)(b)2., a DoD covered entity receives satisfactory assurances from a party seeking PHI if the DoD covered entity receives from such party a written statement and accompanying documentation demonstrating that:

1. The parties to the dispute concerning the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

2. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

(e) For purposes of Paragraph 4.4.e.(1), a qualified protective order concerning the PHI requested under Paragraph 4.4.e.(2) is an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that satisfies both of the following:

1. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested.

2. Requires the return to the DoD covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

(f) Notwithstanding Paragraph 4.4.e.(1)(b), a DoD covered entity may disclose PHI in response to lawful process described in Paragraph 4.4.e.(1)(b) without receiving satisfactory assurance under Paragraphs 4.4.e.(1)(b)1. or 4.4.e.(1)(b)2. if the DoD covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of Paragraph 4.4.e.(1)(c) or to seek a qualified protective order sufficient to meet the requirements of Paragraph 4.4.e.(1)(d).

(2) **Other Uses and Disclosures Under This Paragraph.** The provisions of Paragraph 4.4.e. do not supersede other provisions of Paragraph 4.4. that otherwise permit or restrict uses or disclosures of PHI.

(3) **Relationship to Privacy Act Disclosures Pursuant to the Order of a Court of Competent Jurisdiction.** Under Section 552a(b)(11) of the Privacy Act, a federal agency may disclose Privacy Act-protected information pursuant to the order of a court (i.e., an order that has been reviewed and approved by a judge) of competent jurisdiction. In certain cases, the authority to disclose PHI in response to an order of a court or administrative tribunal may be broader than the related authority under the Privacy Act. In such cases, other Privacy Act rules and procedures, such as the establishment of a routine use permitting disclosure, and where compulsory legal process is concerned, notification of the individual when the process becomes a matter of public record, may also apply. As stated in Paragraph 3.2.d., a disclosure of PHI must be in accordance with both this issuance and the Privacy Act and DoD Privacy Program issuances.

(4) **Administrative or Judicial Proceedings in Relation to Court-Martial Procedures.** Any order from a military judge in connection with any process under Chapter 47 of Title 10, U.S.C., also known and referred to in this issuance as the “Uniform Code of Military Justice (UCMJ),” is an order covered by Paragraph 4.4.e.(1)(a).

f. Standard: Disclosures for Law Enforcement Purposes. A DoD covered entity may disclose PHI for a law enforcement purpose to a law enforcement official if the conditions in Paragraphs 4.4.f.(1) through 4.4.f.(7) are met, as applicable.

(1) **Permitted Disclosures: Pursuant to Process and as Otherwise Required By Law.** A DoD covered entity may disclose PHI:

(a) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to Paragraph 4.4.b.(1)(b) (reports of child abuse and neglect) or 4.4.c.(1) (reports required by law of abuse, neglect, or domestic violence).

(b) In compliance with, and as limited by, the relevant requirements of:

1. A court order, court-ordered warrant, subpoena, or summons issued by a judicial officer.

2. A grand jury subpoena.

3. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, if:

a. The information sought is relevant and material to a legitimate law enforcement inquiry.

b. The request is in writing, specific, and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

c. De-identified information could not reasonably be used.

(2) **Permitted Disclosures: Limited Information for Identification and Location Purposes.** Except for disclosures required by law as permitted by Paragraph 4.4.f.(1)(a), a DoD covered entity may disclose PHI in response to a law enforcement official’s request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, if:

(a) The DoD covered entity discloses only the following information.

1. Name and address.

2. Date and place of birth.

3. Social security number.

4. ABO blood type and rhesus factor.
5. Type of injury.
6. Date and time of treatment.
7. Date and time of death, if applicable.
8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(b) Except as permitted by Paragraph 4.4.f.(2)(a), the DoD covered entity does not disclose for the purposes of identification or location under Paragraph 4.4.f.(2) any PHI related to the individual's deoxyribonucleic acid analysis, dental records, or typing, samples, or analysis of body fluids or tissue.

(3) **Permitted Disclosure: Victims of a Crime.** In addition to disclosures required by law as permitted by Paragraph 4.4.f.(1) or otherwise authorized under this section (such as disclosures for public health activities or disclosures about victims of abuse, neglect, or domestic violence), a DoD covered entity may disclose PHI in response to a law enforcement official's request for such PHI about an individual who is or is suspected to be a victim of a crime (subject to the special rules for sexual assault and domestic abuse under Paragraph 4.4 f.(7)) if:

- (a) The individual agrees to the disclosure; or
- (b) The DoD covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
 1. The law enforcement official represents that such PHI is needed to determine whether a violation of law by a person other than the victim has occurred, and such PHI is not intended to be used against the victim.
 2. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
 3. The disclosure is in the best interests of the individual as determined by the DoD covered entity, in the exercise of professional judgment.

(4) **Permitted Disclosure: Decedents.** A DoD covered entity may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the DoD covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) **Permitted Disclosure: Crime on Premises.** A DoD covered entity may disclose to a law enforcement official PHI that the DoD covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the DoD covered entity.

(6) Permitted Disclosure: Reporting Crime in Emergencies.

(a) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

1. The commission and nature of a crime.
2. The location of such crime or of the victim(s) of such crime.
3. The identity, description, and location of the perpetrator of such crime.

(b) If a covered health care provider believes that the medical emergency described in Paragraph 4.4.f.(6)(a) is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, Paragraph 4.4.f.(6)(a) does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to Paragraph 4.4.c.

(7) Permitted Disclosure: Sexual Assault and Domestic Abuse Cases. In cases in which a victim of sexual assault or domestic abuse elects restricted reporting under DoDI 6495.02 or DoDI 6400.06, the limitations on disclosure under these issuances apply.

g. Standard: Uses and Disclosures About Decedents.

(1) Coroners and Medical Examiners.

(a) A DoD covered entity may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A DoD covered entity that also performs the duties of a coroner or medical examiner may use PHI for the purposes described in this paragraph.

(b) Any official of the DoD authorized to perform functions under the authority of the Armed Forces Medical Examiner System is a medical examiner under Paragraph 4.4.g.(1).

(2) Funeral Directors. A DoD covered entity may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties concerning the decedent. If necessary for funeral directors to carry out their duties, the DoD covered entity may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

(3) Cross References. See also the last sentence of Paragraph 3.2.f. and Paragraph 4.5.h.

h. Standard: Uses and Disclosures for Cadaveric Organ, Eye, or Tissue Donation Purposes. A DoD covered entity may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

i. Standard: Uses and Disclosures for Research Purposes.

(1) **Permitted Uses and Disclosures.** A DoD covered entity may use or disclose PHI for research, regardless of the source of funding of the research, if the requirements of Paragraphs 4.4.i.(1)(a), 4.4.i.(1)(b), or 4.4.i.(1)(c) are met.

(a) **Board Approval of a Waiver of Authorization.** The DoD covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by Paragraph 4.2. for use or disclosure of PHI has been approved by either:

1. An Institutional Review Board (IRB) that:

a. In the case of research conducted or supported by a DoD Component, is established in accordance with Section 219.107 of Title 32, CFR, also known and referred to in this issuance as the “Common Rule;” or

b. In the case of research not conducted or supported by a DoD Component but conducted or supported by another federal agency, is established in accordance with the agency’s regulation comparable to the Common Rule; or

2. A privacy board that:

a. Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual’s privacy rights and related interests.

b. Includes at least one member who is not affiliated with the DoD covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities.

c. Does not have any member participating in a review of any project for which the member has a conflict of interest.

(b) **Reviews Preparatory to Research.** The DoD covered entity obtains representations from the researcher that:

1. Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research.

2. No PHI is to be removed from the DoD covered entity by the researcher in the course of the review.

3. The PHI for which use or access is sought is necessary for the research purposes.

(c) **Research on Decedent’s Information.** The DoD covered entity obtains from the researcher:

1. Representation that the use or disclosure sought is solely for research on the PHI of decedents.

2. Documentation, at the request of the DoD covered entity, evidencing the death of such individuals.

3. Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

(2) **Documentation of Waiver Approval.** For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under Paragraph 4.4.i.(1)(a), the documentation must include all of the following:

(a) **Identification and Date of Action.** A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved.

(b) **Waiver Criteria.** A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

1. The use or disclosure of PHI involves no more than minimal risk to the privacy of the individuals, based on, at least, the presence of the following elements:

a. An adequate plan to protect the identifiers from improper use and disclosure.

b. An adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law.

c. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by this issuance.

2. The research could not practicably be conducted without the waiver or alteration.

3. The research could not practicably be conducted without access to and use of the PHI.

(c) **PHI Needed.** A brief description of the PHI for which use or access has been determined necessary by the IRB or privacy board, in accordance with Paragraph 4.4.i.(2)(b)3.

(d) **Review and Approval Procedures.** A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures of an IRB or privacy board as set forth below:

1. An IRB must follow the requirements of the Common Rule; Subparts B, C, and D of Part 46 of Title 45, CFR, also known and referred to in this issuance as the “Protection of Human Subjects Regulation;” and DoDI 3216.02, including the normal review procedures or

the expedited review procedures in Sections 219.108(b) and 219.110 of the Common Rule or comparable regulation of another federal agency.

2. A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in Paragraph 4.4.i.(1)(a)2.b., and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with Paragraph 4.4.i.(2)(d)3.

3. A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair.

4. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

j. Standard: Uses and Disclosures to Avert Serious Threat to Health or Safety.

(1) **Permitted Disclosures.** A DoD covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose PHI if the DoD covered entity, in good faith, believes the use or disclosure:

(a) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;

(b) Is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the DoD covered entity reasonably believes may have caused serious physical harm to the victim. However, such a use or disclosure may not be made if such statement is made in the course of treatment related to the propensity to commit the criminal conduct that is the basis for the disclosure, or in the course of counseling or therapy, or through a request by the individual to initiate or to be referred for such treatment, counseling, or therapy. In addition, any such disclosure must reveal only the statement by the individual and the PHI described in Paragraph 4.4.f.(2)(a); or

(c) Is necessary for law enforcement authorities to identify or apprehend an individual where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

(2) **Presumption of Good Faith Belief.** A DoD covered entity that uses or discloses PHI pursuant to Paragraph 4.4.j.(1) is presumed to have acted in good faith with regard to a belief described in Paragraph 4.4.j.(1) if the belief is based upon the DoD covered entity's actual

knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

k. Standard: Uses and Disclosures for Specialized Government Functions.

(1) Military Service Personnel.

(a) General Rule. A DoD covered entity (and a covered entity not part of or affiliated with the DoD) may use and disclose the PHI of individuals who are Service members for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. Exceptions pertaining to disclosures to command authorities of PHI involving Service members seeking mental health services and substance abuse education services are outlined in Paragraph 4.4.k.(1)(d). Further guidance is available on the “Military Command Exception” page of the DHA Privacy Office Website. In the event of a disagreement between a commander and a DoD covered entity (including an affiliated health care provider) concerning disclosure of PHI, the DoD covered entity will, before making its determination, seek the advice of the cognizant legal advisor or command counsel, or the cognizant HIPAA privacy officer (designated under Paragraph 7.1.a(1)), or both, as appropriate.

(b) Appropriate Military Command Authorities. For purposes of Paragraph 4.4.k.(1)(a), appropriate military command authorities are:

1. All commanders who exercise authority over an individual who is a Service member, or other person designated by such a commander to receive PHI in order to carry out an activity under the commander’s authority. In the case of a Reserve or National Guard commander who exercises authority over an individual member of the Reserve or National Guard, such commander may designate Reserve or National Guard members who are medical personnel to access, receive, use, or disclose PHI of an individual under the commander’s authority for the purposes of Paragraph 4.4.k.(1)(c); provided, however, that such designee’s access to PHI in a health records system is subject to the terms and conditions applicable to the system or systems to which access is requested.

2. The Secretary of Defense, the Secretary of the Military Department responsible for the Military Service of which the individual is a member, or the Secretary of the DHS in the case of a member of the Coast Guard when the Coast Guard is not operating as a service in the Department of the Navy.

3. Any official delegated authority by a Secretary listed in Paragraph 4.4.k.(1)(b)2. to take an action designed to ensure the proper execution of the military mission.

(c) Purposes for Which the PHI May Be Used or Disclosed. In accordance with Paragraph 4.4.k.(1)(a), the PHI of an individual who is a Service member may be used or disclosed to:

1. Determine the member’s fitness for duty, including but not limited to the member’s compliance with standards and all other activities carried out under the authority of DoDD 1308.1, DoDI 1332.18, DoDI 5210.42, and similar requirements.

2. Determine the member's fitness to perform any particular mission, assignment, order, or duty, including compliance with any actions required as a precondition to performance of such mission, assignment, order, or duty.

3. Inform a commander that one of the notification standards pertaining to the delivery of mental health services as defined in DoDI 6490.08 is applicable as provided in Paragraph 4.4.k.(d).

4. Carry out activities under the authority of DoDD 6490.02E.

5. Report on casualties in any military operation or activity in accordance with applicable military regulations or procedures.

6. Carry out any other activity necessary for the proper execution of the Military Service mission.

(d) Purposes for Which PHI May Not Be Used or Disclosed in the Case of Mental Health Services. DoDI 6490.08 creates a presumption that a DoD covered entity may not notify a command authority when a Service member obtains mental health services, substance abuse education services, or both. Command notification is prohibited unless the presumption is overcome by one of the notification standards listed in Enclosure 2 of DoDI 6490.08.

1. If the presumption against disclosure is overcome, a DoD covered entity is to notify the commander as outlined in DoDI 6490.08.

2. If a DoD covered entity determines that one of the notification standards applies, the DoD covered entity must notify the commander personally or another person specifically designated by the commander for this purpose. The DoD covered entity must disclose the minimum amount of information necessary to satisfy the purpose of the disclosure. In general, this will consist of the diagnosis, the treatment, impact on duty or mission, recommended duty restrictions, the prognosis, and ways the commander can support or assist the Service member's treatment.

(e) Federal Register Notice. The operation of Paragraph 4.4.k.(1)(a) required the publication of a notice in the Federal Register containing the provisions of Paragraphs 4.4.k.(1)(b) and 4.4.k.(1)(c). This information was published for the DoD in the Federal Register Notice dated April 9, 2003, and for the Coast Guard, April 23, 2003. The DoD Federal Register Notice is available on the DHA Privacy Office Website.

(2) Separation or Discharge From Military Service. A DoD covered entity that is a component of the DoD or DHS may disclose to the Department of Veterans Affairs (VA) the PHI of an individual who is a Service member upon the separation or discharge of the individual from military service for the purpose of a determination by VA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of VA. Pursuant to Section 525 of Public Law 113-66, also known as the "National Defense Authorization Act for Fiscal Year 2014," service treatment records will be made available to VA no later than 90 days after the date of the veteran's discharge or release.

(3) **Foreign Military Personnel.** A DoD covered entity may use and disclose the PHI of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Service members under Paragraph 4.4.k.(1).

(4) **National Security and Intelligence Activities.** A DoD covered entity may disclose PHI to authorized DoD and other federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by Section 401 of Title 50, U.S.C. (also known as the “National Security Act”) and implementing authority (e.g., Executive Order 12333).

(5) **Protective Services for the President and Others.** A DoD covered entity may disclose PHI to authorized federal officials for:

(a) The provision of protective services to the President or other persons authorized by Section 3056 of Title 18, U.S.C., or to foreign heads of state or other persons authorized by Section 2709(a)(3) of Title 22 U.S.C.; or

(b) The conduct of investigations authorized by Sections 871 and 879 of Title 18, U.S.C.

(6) **Correctional Institutions and Other Law Enforcement Custodial Situations.**

(a) **Permitted Disclosures.** A DoD covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual PHI about such inmate or individual, if the correctional institution or such law enforcement official represents that such PHI is necessary for:

1. The provision of health care to such individuals.

2. The health and safety of such individual or other inmates.

3. The health and safety of the officers or employees of or others at the correctional institution.

4. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another.

5. Law enforcement on the premises of the correctional institution.

6. The administration and maintenance of the safety, security, and good order of the correctional institution.

(b) **Permitted Uses.** A DoD covered entity that is a correctional institution may use PHI of individuals who are inmates for any purpose for which such PHI may be disclosed.

(c) **No Application After Release.** For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(7) **Covered Entities That Are Government Programs Providing Public Benefits.**

(a) A health plan that is a government program providing public benefits may disclose PHI relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(b) A DoD covered entity that is a government agency administering a government program providing public benefits may disclose PHI relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

1. Standard: Disclosures for Workers Compensation. A DoD covered entity may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

4.5. SPECIAL RULES AND OTHER REQUIREMENTS RELATING TO USES AND DISCLOSURES OF PHI.

a. De-Identification of PHI.

(1) **Standard: Uses and Disclosures of De-Identified PHI.** A DoD covered entity may use PHI to create information that is not individually identifiable health information, or disclose PHI only to a business associate for such purpose, whether or not the de-identified information is to be used by the DoD covered entity. Health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(2) **Implementation Specifications: Requirements for De-Identification of PHI.** A DoD covered entity may determine that health information is not individually identifiable health information only if:

(a) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information, and documents the methods and results of the analysis that justify such determination.

(b) The identifiers listed in Paragraph 4.5.a.(2)(c) of the individual or of relatives, employers, or household members of the individual, are removed and the DoD covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) The identifiers referred to in Paragraph 4.5.a.(2)(b) are:

1. Names.

2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people.

b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

4. Telephone numbers.

5. Fax numbers.

6. Electronic mail addresses.

7. Social security numbers.

8. Medical record numbers.

9. Health plan beneficiary numbers.

10. Account numbers.

11. Certificate or license numbers.

12. Vehicle identifiers and serial numbers, including license plate numbers.

13. Device identifiers and serial numbers.

14. Web Universal Resource Locators.

15. Internet Protocol address numbers.

16. Biometric identifiers, including finger and voice prints.

17. Full-face photographic images and any comparable images.

18. Any other unique identifying number, characteristic, or code, including but not limited to an individual's DoD identification number, except as permitted by Paragraph 4.5.a.(3).

(3) Implementation Specifications: Re-Identification. A DoD covered entity may assign a code or other means of record identification to allow information de-identified under this Paragraph 4.5.a. to be re-identified by the DoD covered entity, if:

(a) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual.

(b) Security. The DoD covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

b. Minimum Necessary Rule.

(1) Standard: Minimum Necessary. When using or disclosing PHI in any form or when requesting PHI from another DoD covered entity or business associate, a DoD covered entity or business associate must make reasonable efforts to limit the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The "reasonable efforts" standard applies to the implementation specifications in Paragraphs 4.5.c. through 4.5.g.

(2) Minimum Necessary Does Not Apply. The minimum necessary rule does not apply to:

- (a) Disclosures to, or requests by, a health care provider for treatment.
- (b) Uses or disclosures made to the individual.
- (c) Uses and disclosures made pursuant to an authorization under Paragraph 4.2.
- (d) Disclosures made to the Secretary of HHS referred to in Paragraph 3.2.c.
- (e) Uses or disclosures that are required by law, as described by Paragraph 4.4.a.
- (f) Uses or disclosures that are required for compliance with this issuance.

(3) Implementation Specifications: Minimum Necessary Uses of PHI.

(a) A DoD covered entity must identify:

1. Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties.

2. For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

(b) A DoD covered entity must make reasonable efforts to limit PHI access of such persons or classes identified in Paragraph 4.5.b.(3)(a)1., consistent with Paragraph 4.5.b.(3)(a)2.

(4) Implementation Specification: Minimum Necessary Disclosures of PHI.

(a) For any type of disclosure that it makes on a routine and recurring basis, a DoD covered entity must implement policies and procedures (may be standard protocols) that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(b) For all other disclosures, a DoD covered entity must:

1. Develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.

2. Review requests for disclosure on an individual basis in accordance with such criteria.

(c) A DoD covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

1. Making disclosures to public officials that are permitted under Paragraph 4.4., if the public official represents that the information requested is the minimum necessary for the stated purpose(s).

2. The information is requested by another covered entity.

3. The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).

4. Documentation or representations that comply with the applicable requirements of Paragraph 4.4.i. have been provided by a person requesting the information for research purposes.

(5) Implementation Specifications: Minimum Necessary Requests for PHI.

(a) When requesting PHI from other covered entities, a DoD covered entity must limit any request to the amount reasonably necessary to accomplish the purpose for which the request is made.

(b) For a request that is made on a routine and recurring basis, a DoD covered entity must implement policies and procedures (may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(c) For all other requests, a DoD covered entity must:

1. Develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made.

2. Review requests for disclosure on an individual basis in accordance with such criteria.

(6) Implementation Specification: Other Content Requirement. For all uses, disclosures, or requests to which the requirements in Paragraph 4.5.b. apply, a DoD covered entity may not use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

c. Limited Data Set.

(1) Standard: Limited Data Set. A DoD covered entity may use or disclose a limited data set that meets the requirements of Paragraphs 4.5.c.(2) and 4.5.c.(3), if the DoD covered entity enters into a data use agreement with the limited data set recipient, in accordance with Paragraph 4.5.c.(4).

(2) Implementation Specification: Limited Data Set. A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- (a) Names.
- (b) Postal address information, other than town or city, State, and zip code.
- (c) Telephone numbers.
- (d) Fax number.
- (e) Electronic mail addresses.
- (f) Social security numbers.
- (g) Medical record numbers.
- (h) Health plan beneficiary numbers.
- (i) Account numbers.
- (j) Certificate or license numbers.
- (k) Vehicle identifiers and serial numbers, including license plate numbers.
- (l) Device identifiers and serial numbers.

- (m) Web Universal Resource Locators.
- (n) Internet Protocol address numbers.
- (o) Biometric identifiers, including finger and voice prints.
- (p) Full-face photographic images and any comparable images.

(3) Implementation Specifications: Permitted Purposes for Uses and Disclosures.

(a) A DoD covered entity may use or disclose a limited data set under Paragraph 4.5.c.(1) for the purposes of research, public health, or health care operations.

(b) A DoD covered entity may use PHI to create a limited data set that meets the requirements of Paragraph 4.5.c.(2), or disclose PHI only to a business associate for such purpose, whether or not the limited data set is to be used by the DoD covered entity.

(4) Implementation Specifications: Data Use Agreement.

(a) **Agreement Required.** A DoD covered entity may use or disclose a limited data set under Paragraph 4.5.c.(1) if the DoD covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this Paragraph 4.5.c.(4), that the limited data set recipient will only use or disclose the PHI for limited purposes.

(b) **Contents.** A data use agreement between the DoD covered entity and the limited data set recipient must:

1. Establish the permitted uses and disclosures of such information by the limited data set recipient consistent with Paragraph 4.5.c.(3). The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate this requirement, if done by the DoD covered entity.

2. Establish who is permitted to use or receive the limited data set.

3. Provide that the limited data set recipient will:

a. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law.

b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided by the data use agreement.

c. Report to the DoD covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware.

d. Ensure that any agents to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information.

- e. Not identify the information or contact the individuals.

(c) **Compliance.**

1. A DoD covered entity is not in compliance with the standards of Paragraph 4.5.c.(1) if the DoD covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the DoD covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

- a. Discontinued disclosure of PHI to the recipient.
- b. Reported the problem to the Secretary of HHS.

2. A DoD covered entity that is a limited data set recipient and violates a data use agreement will be in non-compliance with the standards, implementation specifications, and requirements of Paragraph 4.5.c.

d. Incidental Use and Disclosure Rule.

(1) **Concept.** Subject to the conditions stated in Paragraph 4.5.d.(2), a DoD covered entity is permitted to use or disclose PHI if such use or disclosure is incidental to a use or disclosure otherwise permitted or required by this issuance.

(2) **Requirements for Applying Rule.** The incidental use and disclosure rule applies only when the DoD covered entity has complied with the following:

- (a) The minimum necessary rule under Paragraph 4.5.b. by making reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure, consistent with that paragraph.
- (b) The requirement of Paragraph 7.3.a. by having in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

(3) **Examples of Application of Incidental Uses and Disclosures Rule.** Subject to compliance by a DoD covered entity of the conditions established in Paragraph 4.5.d.(2), the following are examples of incidental uses and disclosures that are permitted under Paragraph 4.5.d.(1):

- (a) Confidential conversations among health care providers or with patients when there is a possibility they may be overheard.
- (b) Using sign-in sheets in waiting rooms or calling patients in waiting rooms by name.
- (c) Posting the patient's name on the wall outside the patient's room.
- (d) Maintaining patient charts at the patient's bedside.

- (e) Placing patient charts outside the examination room.
- (f) Leaving messages for patients on their answering machines or with a family member answering the phone.
- (g) Discussing mental health issues among individuals participating in a group therapy session.
- (h) Using X-ray light boards.
- (i) Discussing a patient's condition during training rounds in connection with a health care professional training program.

(4) **Nonapplicability of the Incidental Uses and Disclosures Rule.** The incidental uses and disclosure rule of Paragraph 4.5.d.(1) does not excuse non-compliance with this issuance due to mistakes, neglect, a failure to have in place appropriate safeguards, or a failure to make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.

e. Standard: Disclosure to Business Associates.

(1) A DoD covered entity may disclose PHI to a business associate and may allow a business associate to create, receive, maintain, or transmit PHI on its behalf, if the DoD covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A DoD covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may disclose PHI to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf, if the business associate obtains satisfactory assurances, in accordance with Paragraph 4.5.e.(1), that the subcontractor will appropriately safeguard the information.

(3) A DoD covered entity must document the satisfactory assurances required by Paragraph 4.5.e.(1) through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of Paragraph 3.3.c.(3). As stated in Paragraph 3.3.c.(1), in the case of a business associate that is a DoD Component and is covered by this issuance, Paragraph 3.3.c.(2) provides the documentation required by this paragraph.

f. Standard: Disclosures by Whistleblowers and Workforce Crime Victims.

(1) **Disclosures by Whistleblowers.** A DoD covered entity is not considered to have violated the requirements of this issuance if a member of its workforce or a business associate discloses PHI, provided:

(a) The workforce member or business associate believes in good faith that the DoD covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the DoD covered entity potentially endangers one or more patients, workers, or the public.

(b) The disclosure is to:

1. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the DoD covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the DoD covered entity; or

2. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in Paragraph 4.5.f.(1)(a).

(2) **Disclosures by Workforce Members Who Are Victims of a Crime.** A DoD covered entity is not considered to have violated the requirements of this issuance if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official, provided that the PHI disclosed is:

(a) About the suspected perpetrator of the criminal act.

(b) Limited to the identification information listed in Paragraph 4.4.f.(2)(a).

g. Personal Representatives.

(1) **Standard: Personal Representatives.** As specified in this paragraph, a DoD covered entity must, except as provided in Paragraphs 4.5.g.(3) and 4.5.g.(5), treat a personal representative as the individual for purposes of this issuance.

(2) **Implementation Specification: Adults and Emancipated Minors.** If, under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a DoD covered entity must treat such person as a personal representative under this issuance regarding PHI relevant to such personal representation.

(3) **Implementation Specification: Unemancipated Minors.**

(a) If, under applicable law, a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a DoD covered entity must treat such person as a personal representative under this issuance regarding PHI relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, regarding PHI pertaining to a health care service, if:

1. The minor provides informed consent to such health care service; no other informed consent to such health care service is required by law, regardless of whether the informed consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

2. The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

3. A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(b) Notwithstanding the provisions of Paragraph 4.5.g.(3)(a):

1. To the extent permitted or required by an applicable provision of State or other law, including applicable case law, a DoD covered entity may disclose, or provide access in accordance with Paragraph 5.3. to, PHI about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*.

2. To the extent prohibited by an applicable provision of State or other law, including applicable case law, a DoD covered entity may not disclose, or provide access to, PHI about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis* in accordance with Paragraph 5.3.

3. Where the parent, guardian, or other person acting *in loco parentis* is not the personal representative under Paragraphs 4.5.g.(3)(a)1., 4.5.g.(3)(a)2., or 4.5.g.(3)(a)3., and where there is no applicable access provision under State or other law, including case law, a DoD covered entity may provide or deny access under Paragraph 5.3. to a parent, guardian, or other person acting *in loco parentis* if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional in the exercise of professional judgment.

(c) Notwithstanding the provisions of Paragraph 4.5.g.(3)(a), a DoD covered entity must, consistent with State or other applicable law, provide a right of access, as set forth in Paragraph 5.3. to either a parent, guardian, or other person acting *in loco parentis* as the personal representative of the unemancipated minor, the unemancipated minor, or both.

(4) **Implementation Specification: Deceased Individuals.** If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or the individual's estate, a DoD covered entity must treat such person as a personal representative under this issuance regarding PHI relevant to such personal representation.

(5) **Implementation Specification: Abuse, Neglect, Endangerment Situations.** Notwithstanding a State law or any requirement of this issuance to the contrary, a DoD covered entity may elect not to treat a person as the personal representative of an individual if:

(a) The DoD covered entity has a reasonable belief that:

1. The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

2. Treating such person as the personal representative could endanger the individual.

(b) The DoD covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

h. Standard: Deceased Individuals. A DoD covered entity must comply with the requirements of this issuance regarding the PHI of a deceased individual for a period of 50 years following the death of the individual.

(1) A DoD covered entity may be required by law to disclose certain documents under FOIA. As such, there may be certain circumstances whereby the HIPAA Privacy Rule and this issuance may not prevent the disclosure of PHI of deceased individuals during the 50 year period following the death of an individual. However, FOIA is more limited in scope. It generally does not protect the records and privacy of deceased individuals, but it does offer an exemption (exemption 6) which may in some cases be used to protect the privacy of other individuals such as the deceased persons surviving family members.

(2) As set forth in Paragraph 1.1.b.(9), the Armed Forces Medical Examiner System is not subject to the requirements of this issuance and may release death certificates and autopsy reports without regard to the provisions of this issuance.

(3) Covered entities must evaluate each disclosure regarding deceased individuals on a case-by-case basis.

i. Verification of Identity Before Disclosure of PHI.

(1) **Standard: Verification Required.** Before a disclosure authorized by this issuance is made, a DoD covered entity must verify the identity of any person or entity requesting PHI and the authority of any such person or entity to have access to the requested PHI, if the identity or such authority is not known to the DoD covered entity. The DoD covered entity must obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of disclosure under this issuance.

(2) **Implementation Specification: Conditions on Disclosures.**

(a) **Reasonable Reliance.** If a disclosure under this issuance is conditioned by this paragraph on particular documentation, statements, or representations from the person requesting the PHI, a DoD covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

1. The conditions in Paragraph 4.4.f.(1)(b)3. may be satisfied by an administrative subpoena or similar process or by a separate written statement that, on its face, specifically demonstrates that the applicable requirements have been met.

2. The documentation required by Paragraph 4.4.i.(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with Paragraph 4.4.i.(2).

(b) **Individual Requests.** Individuals may request release of their PHI to either themselves or to other individuals they have authorized. In these circumstances, the individual's identity must be verified by the DoD covered entity before any disclosure.

1. The following documents may be used to verify the identity of the individual:

- a. Military identification card.
- b. Individual's driver's license.
- c. Employment identification card or badge.
- d. Passport.
- e. Other government issued identification.

2. If the individual's name has been legally changed, evidence documenting the name change must be presented.

(c) **Public Official Requests.**

1. **Identity of Public Officials.** A DoD covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

a. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status.

b. If the request is in writing, the request is on the appropriate government letterhead.

c. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

2. **Authority of Public Officials.** A DoD covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

a. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority.

b. A request made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal (such a request is presumed to constitute legal authority).

3. Exercise of Professional Judgment. The verification requirements specified above are met if the DoD covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with Paragraph 4.3. or acts based upon a good faith belief in making a disclosure in accordance with Paragraph 4.4.j.

j. Special Rules for Substance Use Disorder Records. Covered entities must comply with the special rules protecting the confidentiality of substance use disorder patient records in federally assisted substance use disorder programs. Those rules are under the authority of the Substance Abuse and Mental Health Services Administration and appear at Part 2 of Title 42, CFR. To the extent those rules apply to PHI of the DoD covered entity:

(1) The DoD covered entity must comply with both those rules and this issuance. To the extent any use or disclosure is authorized by this issuance but prohibited by Part 2 of Title 42, CFR, the prohibition will control.

(2) For any use or disclosure that is authorized by Part 2 of Title 42, CFR, but prohibited by this issuance, the prohibition will control. Covered substance use disorder patient records may only be used or disclosed if the requirements of both this issuance and Part 2 of Title 42, CFR, are satisfied.

k. Special Rules for Genetic Information. Notwithstanding any other provision of this issuance, a health plan must not use or disclose PHI that is genetic information for underwriting purposes. This prohibition overrides any individual authorization of such use or disclosure. Information on what is considered to be genetic information subject to the limitation of this Paragraph 4.5.k. may be found in the HIPAA Privacy Rule.

SECTION 5. RIGHTS OF INDIVIDUALS

5.1. NOTICE OF PRIVACY PRACTICES (NOPP) FOR PHI.

a. Standard: NoPP.

(1) **Right to Notice.** Except as provided by Paragraph 5.1.a.(2), an individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the DoD covered entity, and of the individual's rights and the DoD covered entity's legal duties with respect to PHI.

(2) **Exception for Inmates.** An inmate does not have a right to notice under this paragraph, and the requirements of this paragraph do not apply to a correctional institution that is a DoD covered entity.

(3) **Uses and Disclosures Consistent With Notice.** A DoD covered entity that is required to have a notice under Paragraph 5.1.a.(1) may not use or disclose PHI in a manner inconsistent with the notice.

b. Implementation Specifications: Content of MHS NoPP.

(1) **Single MHS NoPP.** The MHS must provide the same NoPP for both its health plans and providers. The MHS NoPP is issued through the DHA.

(2) **Revisions to the Notice.** DHA must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the DoD covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented before the effective date of the notice that reflects the material change. A DoD covered entity, including an MTF, may establish local policies and procedures that strengthen the principles contained in the MHS NoPP, but it cannot amend or change the MHS NoPP itself.

c. Implementation Specifications: Provision of MHS NoPP. A DoD covered entity must make the notice required by this paragraph available on request to any person and to individuals as specified in Paragraphs 5.1.c.(1) through 5.1.c.(3)(d), as applicable.

(1) Specific Requirements for Health Plans.

(a) A health plan must provide notice no later than the compliance date for the health plan, to individuals then covered by the plan. Thereafter the plan must provide notice:

1. To individuals who newly become covered by the plan at the time or prior to the time they become covered.

2. Within 60 days of a material revision to the notice, to individuals then covered by the plan.

(b) No less frequently than once every 3 years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(c) The health plan satisfies the requirements of Paragraph 5.1.c.(1) if notice is provided to the sponsor under coverage.

(2) **Specific Requirements for Certain Covered Health Care Providers.** A covered health care provider that has a direct treatment relationship with an individual must:

(a) **Provide the notice:**

1. To the individual no later than the date of first service delivery, including service delivered electronically; or

2. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(b) **Obtain Acknowledgement of Receipt:**

1. Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with Paragraph 5.1.c.(2)(a) at the individual's first encounter for care. An MHS facility is not required to repeat the NoPP acknowledgement process after the individual's first encounter for care at that MHS facility.

a. The individual or the individual's representative should, but is not required to, sign the acknowledgement of NoPP receipt.

b. If the individual or the individual's representative refuses to sign the acknowledgement, the covered health care provider must document the good faith effort to obtain the acknowledgement and the reason why the acknowledgement was not obtained.

2. If the covered entity health care provider maintains a physical service delivery site, it will:

a. Have the notice available at the service delivery site for individuals to take with them upon request.

b. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the DoD covered entity health care provider, to be able to read the notice.

c. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of Paragraph 5.1.c.(2), if applicable.

(3) **Specific Requirements for Electronic Notice.**

(a) A DoD covered entity that maintains a website that provides information about the DoD covered entity's customer services or health benefits must prominently post its notice on the website and make the notice available electronically through the website.

(b) A DoD covered entity may provide the notice required by Paragraph 5.1.c.(3) to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the DoD covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Providing the notice electronically will satisfy the requirements of Paragraph 5.1.c. when made in a timely manner and in accordance with Paragraphs 5.1.c.(1) or 5.1.c.(2).

(c) For purposes of Paragraph 5.1.c.(2)(a), if an individual's first encounter for care is delivered electronically, the covered health care provider must automatically provide the available NoPP electronically in response to the individual's first request for service. The covered health care provider must make a good faith effort to obtain written acknowledgement of the individual's electronic receipt of the NoPP as soon as it is reasonably practicable, or document its efforts to obtain such and the reason why it was not obtained, as provided in Paragraph 5.1.c.(2)(b).

(d) The individual who is the recipient of an electronic notice retains the right to obtain a paper copy of the notice from a DoD covered entity upon request.

d. Implementation Specifications: Joint Notice by Separate Covered Entities. All DoD covered entities that are components of the MHS (and thus participate in that organized health care arrangement) must comply with this paragraph by a joint notice.

(1) The DoD covered entities of the MHS must abide by the terms of the notice with respect to PHI created or received by the DoD covered entity as part of its participation in the organized health care arrangement.

(2) The DoD covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of Paragraph 5.1.c. Provision of the joint notice to an individual by any one of the DoD covered entities included in the joint notice satisfies the provision requirement of Paragraph 5.1.c. regarding all others covered by the joint notice.

e. Implementation Specifications: Documentation. A DoD covered entity must document compliance with the notice requirements in Paragraph 5.1.c.(2) by retaining copies of the notices issued by the DoD covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with Paragraph 5.1.c.(2).

5.2. RIGHTS TO REQUEST PRIVACY PROTECTION FOR PHI.

a. Right to Request Restriction.

(1) Standard: Right of an Individual to Request Restriction of Uses and Disclosures.

(a) A DoD covered entity must permit an individual to request that the DoD covered entity restrict:

1. Uses or disclosures of PHI about the individual to carry out treatment, payment, or health care operations.

2. Disclosures permitted under Paragraph 4.3.b.

(b) A DoD covered entity is not required to agree to a restriction except as provided in Paragraph 5.2.a.(1)(g).

(c) The decision whether to agree to a restriction requested by an individual is subject to the discretion of the DoD covered entity. The restriction should be denied if the DoD covered entity cannot reasonably accommodate the request, if it conflicts with this issuance, or for other appropriate reasons.

(d) A DoD covered entity that agrees to a restriction under Paragraph 5.2.a.(1)(a) may not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the DoD covered entity may use the restricted PHI, or may disclose such information to a health care provider, to provide such treatment to the individual.

(e) If restricted PHI is disclosed to a health care provider for emergency treatment under Paragraph 5.2.a.(1)(d), the DoD covered entity must request that such health care provider not use or disclose the information further.

(f) A restriction agreed to by a DoD covered entity under Paragraph 5.2.a.(1)(a) is not effective under this paragraph to prevent uses or disclosures permitted or required under Paragraph 4.3.a., Paragraph 4.4., Paragraph 5.3., or Paragraph 5.5.

(g) A DoD covered entity must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if:

1. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law.

2. The PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the DoD covered entity in full.

(h) DoD covered entities must direct individuals seeking to request restrictions under Paragraph 5.2.a.(1) to submit their request, orally or in writing, to the person or office that would be obliged to comply with the restriction. For example, if compliance would only be required by an MTF, the request must be made in accordance with standard procedures at that MTF and may not be transferred to another MTF. If compliance would be required of the entire MHS, the request must be made to the DHA Privacy Office. No restriction will be effective above the management authority level that agreed to the restriction and no restriction will be effective

unless the person agreeing to the restriction is actually authorized to agree to it and establishes a written record of the restriction.

1. The deciding official for the most senior management authority that would be required to comply with the restriction must determine whether the request will be agreed to, notify the person making the request of the decision in writing as soon as practicable, and take any appropriate implementation action, including establishing a written record of the restriction. If the requested restriction is denied in whole or in part, the notification must include the rationale for the denial.

2. Communication of an agreed upon restriction must be made to all workforce members of the DoD covered entity who might make a disclosure of the individual's restricted PHI. All restriction requests, along with the approval or denial of the request, must be recorded to allow for tracking of the restriction.

(2) Implementation Specifications: Terminating a Restriction. A DoD covered entity may terminate a restriction, if:

- (a) The individual agrees to or requests the termination in writing.
- (b) The individual orally agrees to the termination and the oral agreement is documented.
- (c) The DoD covered entity informs the individual in writing that it is terminating its agreement to a restriction and documents that the individual has been informed of the termination, except that any such termination is:
 - 1. Not effective for PHI restricted under Paragraph 5.2.a.(1)(g).
 - 2. Only effective for PHI created or received after the DoD covered entity has informed the individual of the termination.

(3) Implementation Specification: Documentation. A DoD covered entity must document the restriction in accordance with Paragraph 7.3.d. Oral and written requests for restriction of PHI may be documented on DD Form 2871, "Request to Restrict Medical or Dental Information." The form is available on the DHA Privacy Office Website. However, this form must not be used to request restrictions on the use and disclosure of PHI resulting from a substance use disorder program.

b. Right to Request Confidential Communications.

(1) Standard: Confidential Communications Requirements.

(a) A covered health care provider must permit individuals to request, and must accommodate reasonable requests by individuals to receive, communications of PHI from the covered health care provider by alternative means or at alternative locations.

(b) A health plan must permit and accommodate reasonable requests by individuals to receive communications of PHI from the health plan by alternative means or at alternative locations. The individual must clearly state that the disclosure of all or part of that information could endanger the individual.

(2) Implementation Specifications: Conditions on Providing Confidential Communications. A DoD covered entity:

(a) May require the individual to make a written request for confidential communication described in Paragraph 5.2.b.(1).

(b) Must document requests for confidential communications or the DoD covered entity's responses to such requests in accordance with Paragraph 7.3.d.

(c) May condition the provision of a reasonable accommodation on:

1. Information as to how payment, if any, will be handled.

2. Specification of an alternative address or other method of contact such as telephone or e-mail.

(d) When the covered entity is a health care provider, it must not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(e) When the covered entity is a health plan, it may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

5.3. ACCESS OF INDIVIDUALS TO PHI.

a. Standard: Access to PHI.

(1) **Right of Access.** Except as otherwise provided in Paragraph 5.3.a.(2) or 5.3.a.(3), an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set.

(2) **Unreviewable Grounds for Denial.** Subject to Paragraph 5.3.a.(4), a DoD covered entity may deny an individual access without providing the individual an opportunity for review, with respect to the following information in a designated record set:

(a) Psychotherapy notes.

(b) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(c) Quality assurance information that may not be disclosed under Section 1102 of Title 10, U.S.C., and DoDI 6025.13.

(d) A DoD covered entity that is a correctional institution or a covered health care provider acting under the direction of a correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(e) An individual's access to PHI created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, if the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(f) An individual's access to PHI that is contained in records that are subject to the Privacy Act may be denied, if the denial of access under the Privacy Act would meet the requirements of that law. Examples of records for which access may be denied pursuant to certain exemptions available under the Privacy Act include records classified in the interest of national defense or foreign policy and certain investigatory material.

(g) An individual's access may be denied if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) **Reviewable Grounds for Denial.** A DoD covered entity may deny an individual access, if the individual is given a right to have such denials reviewed, as required by Paragraph 5.3.a.(5), under the following circumstances:

(a) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(b) The PHI makes reference to another person, unless such other person is a health care provider, and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(c) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) **Relationship to the Privacy Act.** The Privacy Act generally gives individuals unqualified access to their information in systems of records maintained by federal agencies. In some cases, PHI that is subject to a request for access covered by this issuance is also subject to the access rules of the Privacy Act. In such cases, access will generally be granted by the DoD covered entity unless the PHI is withheld pursuant to both the provisions of this issuance (Paragraph 5.3.a.(2) or 5.3.a.(3)) and DoD Privacy Program issuances. In the event of a

disagreement between a DoD covered entity (including an affiliated health care provider) and a requestor concerning the disclosure of PHI, the DoD covered entity must seek the advice of the cognizant legal advisor or command counsel, the cognizant HIPAA privacy officer (designated under Paragraph 7.1.a.(1)), or both, as appropriate.

(5) **Review of a Denial of Access.** If access is denied as permitted under Paragraph 5.3.a.(3), the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the DoD covered entity to act as a reviewing official and who did not participate in the original decision to deny. The DoD covered entity must provide or deny access in accordance with the determination of the reviewing official under Paragraph 5.3.d.(4).

b. Implementation Specifications: Requests for Access and Timely Action.

(1) **Individual's Request for Access.** A DoD covered entity must permit an individual to request access to inspect or obtain a copy of the PHI about the individual that is maintained in a designated record set. Audit logs or access reports, which provide information on who has accessed PHI, are not part of a designated record set. The DoD covered entity may require individuals to make requests for access in writing, if it informs individuals of such a requirement.

(2) **Timely Action by the DoD Covered Entity.**

(a) Except as provided in Paragraph 5.3.b.(2)(b), the DoD covered entity must act on a request for access no later than 30 days after receipt of the request as set forth in this paragraph.

1. If the DoD covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested in accordance with Paragraph 5.3.c.

2. If the DoD covered entity denies the request, in whole or in part, it must provide the individual with a written denial in accordance with Paragraph 5.3.d.

(b) If the DoD covered entity is unable to take an action required by Paragraph 5.3.b.(2)(a)1. or 5.3.b.(2)(a)2. within the time required by Paragraph 5.3.b.(2)(a)1., or 5.3.b.(2)(a)2. as applicable, the DoD covered entity may extend the time for such actions by no more than 30 days.

1. The DoD covered entity, within the time limit set by Paragraph 5.3.b.(2)(a) must provide the individual with a written statement of the reasons for the delay and the date by which the DoD covered entity must complete its action on the request.

2. The DoD covered entity may have only one such extension of time for action on a request for access.

c. Implementation Specifications: Provision of Access. If the DoD covered entity provides an individual with access, in whole or in part, to PHI, the DoD covered entity must comply with the following requirements:

(1) **Providing the Access Requested.** The DoD covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the PHI about them in designated record sets. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the DoD covered entity need only produce the PHI once in response to a request for access.

(2) **Form of Access Requested.**

(a) The DoD covered entity must provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form and format as agreed to by the DoD covered entity and the individual.

(b) Notwithstanding Paragraph 5.3.c.(2)(a), if the requested PHI is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the DoD covered entity must provide the individual with access to the PHI in the requested electronic form if it is readily producible. If the PHI cannot be produced in the requested format, it must be in a readable form and format as agreed to by the DoD covered entity and the individual.

(c) The DoD covered entity may provide the individual with a summary of the PHI requested, instead of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to:

1. Such a summary or explanation.
2. The fees imposed, if any, by the DoD covered entity for such summary or explanation.

(d) **Time and Manner of Access.**

1. The DoD covered entity must provide the access as requested by the individual in a timely manner as required by Paragraph 5.3.b.(2), including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request. The DoD covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

2. If an individual's request for access directs the DoD covered entity to transmit the copy of PHI directly to another person designated by the individual, the DoD covered entity must provide the copy to the designated person. The individual's request must be in writing and signed by the individual. The written request must clearly identify the designated person and where to send the copy of the PHI.

(e) **Fees.** If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, the DoD covered entity may impose a reasonable, cost-based fee in accordance with any applicable Military Service or DHA guidance, if the fee includes only the cost of:

1. Labor for copying the PHI requested by the individual, whether in paper or electronic form.

2. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media, provided that copying to portable media is permitted only in accordance with DoD guidance (for example, copying from DoD systems to a USB device is not permitted).

3. Postage, when the individual has requested the copy, or the summary or explanation, be mailed.

4. Preparing an explanation or summary of the PHI, if agreed to by the individual as required by Paragraph 5.3.c.(2)(c).

d. Implementation Specifications: Denial of Access. If the DoD covered entity denies access, in whole or in part, to PHI, the DoD covered entity must comply with the following requirements.

(1) **Making Other Information Accessible.** The DoD covered entity must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI that the DoD covered entity has a ground to deny.

(2) **Denial.** The DoD covered entity must provide a timely written denial to the individual, in accordance with Paragraph 5.3.b.(2). The denial must be in plain language and contain:

(a) The basis for the denial.

(b) If applicable, a statement of the individual's review rights under Paragraph 5.3.a.(4), including a description of how the individual may exercise such review rights.

(c) A description of how the individual may complain to the DoD covered entity pursuant to the complaint procedures in Paragraph 7.2.a. or to the Secretary of HHS pursuant to the procedures in Section 160.306 of the HIPAA Enforcement Rule. The description must include the name, title, and telephone number of the contact person or office designated in Paragraph 7.1.a.(1)(b).

(3) **Other Responsibility.** If the DoD covered entity does not maintain the requested PHI, and the DoD covered entity knows where it is maintained, the DoD covered entity must inform the individual where to direct the request for access.

(4) **Review of Denial Requested.** If the individual has requested a review of a denial under Paragraph 5.3.a.(5), the DoD covered entity must designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access. The DoD covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in Paragraph 5.3.a.(3). The

DoD covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this issuance to carry out the designated reviewing official's determination.

e. Implementation Specifications: Documentation. A DoD covered entity must document the following and retain the documentation as required by Paragraph 7.3.d.:

- (1) The designated record sets that are subject to access by individuals.
- (2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

5.4. AMENDMENT OF PHI.

a. Standard: Right to Amend.

(1) **Right to Amend.** An individual has the right to have a DoD covered entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

(2) **Denial of Amendment.** A DoD covered entity may deny an individual's request for amendment, if it determines that the subject PHI or record that is the subject of the request:

- (a) Was not created by the DoD covered entity, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
- (b) Is not part of the designated record set;
- (c) Would not be available for inspection under Paragraph 5.3; or
- (d) Is accurate and complete.

b. Implementation Specifications: Requests for Amendment and Timely Action.

(1) **Individual's Request for Amendment.** The DoD covered entity must permit an individual to request that the DoD covered entity amend the PHI maintained in the designated record set. The DoD covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, if it informs individuals in advance of such requirements.

(2) Timely Action by the DoD Covered Entity.

(a) The DoD covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request as follows.

1. If the DoD covered entity grants the requested amendment, in whole or in part, it must take the actions required by Paragraphs 5.4.c.(1) and 5.4.c.(2).

2. If the DoD covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial in accordance with Paragraph 5.4.d.(1).

(b) If the DoD covered entity is unable to act on the amendment within the time required by Paragraph 5.4.b.(2), the DoD covered entity may extend the time for such action by no more than 30 days:

1. The DoD covered entity, within the time limit set by Paragraph 5.4.b.(2)(a), must provide the individual with a written statement of the reasons for the delay and the date by which the DoD covered entity must complete its action on the request.

2. The DoD covered entity may have only one such extension of time for action on a request for an amendment.

c. Implementation Specifications: Accepting the Amendment. If the DoD covered entity accepts the requested amendment, in whole or in part, the DoD covered entity must comply with the following requirements.

(1) **Making the Amendment.** The DoD covered entity must make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) **Informing the Individual.** In accordance with Paragraph 5.4.b., the DoD covered entity must provide the individual with a timely, written acceptance and obtain the individual's identification of, and agreement to have the DoD covered entity notify, the relevant persons to be informed under Paragraph 5.4.c.(3).

(3) **Informing Others.** The DoD covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(a) Persons identified by the individual as having received PHI about the individual and needing the amendment.

(b) Persons, including business associates, that the DoD covered entity knows have the subject PHI and whose reliance on the subject PHI may be to the detriment of the individual.

d. Implementation Specifications: Denying the Amendment. If the DoD covered entity denies the requested amendment, in whole or in part, the DoD covered entity must comply with the following requirements:

(1) **Denial.** The DoD covered entity must provide the individual with a timely written denial in accordance with Paragraph 5.4.b.(2)(b). The denial must use plain language and contain:

(a) The basis for the denial, in accordance with Paragraph 5.4.a.(2).

(b) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.

(c) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the DoD covered entity provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment.

(d) A description of how the individual may utilize the complaint procedures established in Paragraph 7.2.a. and in Section 160.306 of the HIPAA Enforcement Rule. The description must include the name, or title, and telephone number of the contact person or office designated in Paragraph 7.1.a.(1)(b). For complaints to the DoD covered entity, individuals will adhere to Paragraph 7.2.a. Complaints to the Secretary of HHS will be made in accordance with Section 160.306 of the HIPAA Enforcement Rule.

(2) **Statement of Disagreement.** The DoD covered entity must permit the individual to submit to the DoD covered entity a written statement disagreeing with the denial of all, or part, of a requested amendment and the basis of such disagreement. The DoD covered entity may reasonably limit the length of a statement of disagreement.

(3) **Rebuttal Statement.** The DoD covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the DoD covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) **Recordkeeping.** The DoD covered entity must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the DoD covered entity's denial of the request, the individual's statement of disagreement, if any, and the DoD covered entity's rebuttal, if any, to the designated record set.

(5) **Future Disclosures**

(a) If a statement of disagreement has been submitted by the individual, the DoD covered entity must include the material appended in accordance with Paragraph 5.4.d.(4), or, at the election of the DoD covered entity, an accurate summary of any such information, with any subsequent disclosure of the PHI relating to the disagreement.

(b) If the individual has not submitted a written statement of disagreement, the DoD covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action in accordance with Paragraph 5.4.d.(1)(c).

(c) When a subsequent disclosure described in Paragraph 5.4.d.(5)(a) or 5.4.d.(5)(b) is made using a standard transaction under Part 162 of Title 45, CFR, that does not permit the additional material to be included with the disclosure, the DoD covered entity may separately transmit the material required by Paragraph 5.4.d.(5)(a) or 5.4.d.(5)(b), as applicable, to the recipient of the standard transaction.

e. Implementation Specifications: Actions on Notices of Amendment. A DoD covered entity that is informed by another DoD covered entity of an amendment to an individual's PHI, in accordance with Paragraph 5.4.c.(3), must amend the PHI in designated record sets as provided by Paragraph 5.4.c.(1).

f. Implementation Specifications: Documentation. A DoD covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by Paragraph 7.3.d.

g. Relationship to the Privacy Act. The Privacy Act also has provisions (Section 552a(d)(2) of Title 5, U.S.C.) regarding amendment of Privacy Act-protected information. If PHI is subject to both this paragraph and Privacy Act requirements, the Privacy Act requirements must continue to apply to matters of amendment according to such requirements.

5.5. ACCOUNTING OF DISCLOSURES OF PHI.

a. Standard: Right to an Accounting of Disclosures of PHI.

(1) An individual has a right to receive an accounting of disclosures of PHI made by a DoD covered entity in the 6 years prior to the date that the accounting is requested, except for disclosures:

(a) To carry out treatment, payment, and health care operations as provided in Paragraph 4.1.

(b) To individuals of PHI about them.

(c) Pursuant to an authorization under Paragraph 4.2.

(d) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in Paragraph 4.3.

(e) For national security or intelligence purposes as provided in Paragraph 4.4.k.(4).

(f) To correctional institutions or law enforcement officials as provided in Paragraph 4.4.k.(6).

(g) As part of a limited data set in accordance with Paragraph 4.5.c.

(h) Incident to use or disclosure otherwise permitted or required by this issuance, as provided in Paragraph 4.5.d.

(i) That occurred prior to the compliance date for the DoD covered entity.

(2) The DoD covered entity must take the following actions under the circumstances stated:

(a) The DoD covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in Paragraph 4.4.d. or 4.4.f., respectively, for the time specified by such agency or official, if such agency or official provides the DoD covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time that such a suspension is required.

(b) If the agency or official statement in Paragraph 5.5.a.(2)(a) is made orally, the DoD covered entity must:

1. Document the statement, including the identity of the agency or official making the statement.

2. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement.

3. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to Paragraph 5.5.a.(2)(a) is submitted during that time.

(c) An individual may request an accounting of disclosures for a period of time less than 6 years from the date of the request.

b. Implementation Specifications: Content of Accounting. The DoD covered entity must provide the individual with a written accounting that meets the following requirements:

(1) Except as otherwise provided by Paragraph 5.5.a., the accounting must include disclosures of PHI that occurred during the 6 years (or such shorter time period at the request of the individual as provided in Paragraph 5.5.a.(2)(c)) prior to the date of the request for an accounting, including disclosures to or by business associates of the DoD covered entity.

(2) Except as otherwise provided by Paragraph 5.5.b.(3) or 5.5.b.(4), the accounting for each disclosure must include:

(a) The date of the disclosure.

(b) The name of the entity or person who received the PHI and, if known, the address of such entity or person.

(c) A brief description of the PHI disclosed.

(d) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement, a copy of a written request for disclosure under Paragraph 3.2.c. or Paragraph 4.4., if any.

(3) If, during the period covered by the accounting, the DoD covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose under

Paragraph 3.2.c.(4)(c) or 4.4., the accounting may, with respect to such multiple disclosures, provide the following:

(a) The information required by Paragraph 5.5.b.(2)(b), for the first disclosure during the accounting period.

(b) The frequency, periodicity, or number of the disclosures made during the accounting period.

(c) The date of the last disclosure during the accounting period.

(4) If, during the period covered by the accounting, the DoD covered entity has made disclosures of PHI for a particular research purpose in accordance with Paragraph 4.4.i. for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

(a) The name of the protocol or other research activity.

(b) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records.

(c) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period.

(d) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed.

(e) A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

(5) If the DoD covered entity provides an accounting for research disclosures in accordance with Paragraph 5.5.b.(4) and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the DoD covered entity must, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

c. Implementation Specification: Provision of Accounting.

(1) The DoD covered entity must act on the individual's request for an accounting within 60 days of request receipt.

(a) The DoD covered entity must provide the individual with the accounting requested.

(b) If the DoD covered entity is unable to provide the accounting within the time required by Paragraph 5.5.c.(1), the DoD covered entity may extend the time to provide the accounting by no more than 30 days.

1. The DoD covered entity, within the time limit set by Paragraph 5.5.c.(1), must provide the individual with a written statement of the reasons for the delay and the date by which the DoD covered entity must provide the accounting.

2. The DoD covered entity may have only one such extension of time for action on a request for an accounting.

(2) The DoD covered entity must provide the first accounting to an individual in any 12-month period without charge. The DoD covered entity may impose a reasonable, cost-based fee in accordance with Service regulations for each subsequent request for an accounting by the same individual within a 12-month period, if the DoD covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

d. Implementation Specification: Documentation. A DoD covered entity must document the following and retain the documentation as required by Paragraph 7.3.d.:

(1) The information required to be included in an accounting under Paragraph 5.5.b. for disclosures of PHI that are subject to an accounting under Paragraph 5.5.a.

(2) The written accounting that is provided to the individual under this paragraph.

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

e. Relationship to the Privacy Act. The Privacy Act also has provisions (Section 552a(c) of Title 5, U.S.C.) requiring an accounting of certain disclosures of Privacy Act protected information. In any case that PHI disclosures are subject to both this paragraph and Privacy Act requirements, Privacy Act requirements must continue to apply to the disclosures according to such requirements.

SECTION 6: BREACH RESPONSE

6.1. BREACH RESPONSE OBLIGATIONS.

a. Requirement. The requirements of this section apply to DoD covered entities and their business associates when they discover a breach of PHI. This section establishes requirements for government reporting, breach assessment, individual notification, and mitigation. The mitigation requirement for business associates includes a requirement to bear the costs to affected individuals and the DoD covered entity resulting from a breach. DoD covered entities and their business associates must comply with the requirements outlined in this section when they discover a breach of PHI. This section:

(1) Implements Section 13402 of the HITECH Act and the HIPAA Breach Rule.

(2) Applies the HIPAA Breach Rule in conjunction with DoD breach response requirements. See Paragraph 6.2.a. and the Glossary definitions of breach/DoD breach, DoD breach response requirements, and HHS breach.

b. DHA Privacy Office Roles and Authority.

(1) Guidance.

(a) The DHA Privacy Office must supplement this section by providing specific operational guidance. This operational guidance must inform DoD covered entities and business associates how to conduct the initial breach reporting and assessments required by the DoD covered entity or business associate.

(b) The DHA Privacy Office has authority to establish different operational requirements for DHA program offices, the Military Departments, DHA contractors, and both purchased care and non-purchased care contractors.

(c) All DoD covered entities and business associates have the authority to establish internal operational procedures to comply with the reporting requirements outlined in this issuance.

(2) Oversight.

(a) The DHA Privacy Office must oversee breach response compliance by DoD covered entities and business associates for each discovered breach, as provided in Paragraph 6.2.

(b) All DoD covered entities and business associates, in responding to discovered breaches, are required to follow DHA Privacy Office determinations. These DHA Privacy Office determinations are subject to review by the Director, DHA, but otherwise take precedence over any contrary decisions by the Military Departments or DHA program offices.

6.2. BREACH RESPONSE PROCEDURES.

a. Overview. When a DoD breach constitutes an HHS breach, complying with this section (taking into account all related operational guidance from the DHA Privacy Office), in addition to the DoD breach response requirements, will satisfy the HIPAA Breach Rule.

b. Initial Reporting.

(1) For all discovered breaches of PHI, the DoD covered entity or business associate must report discovery of the breach to the DHA Privacy Office within 24 hours of discovery of such breach, in addition to breach response and reporting requirements in applicable Office of Management and Budget guidance, DoD Privacy Program issuances, and as prescribed by the Directorate of Oversight and Compliance, including the Defense Privacy, Civil Liberties, and Transparency Division.

(2) In addition to DoD Privacy breach reporting requirements, DoD covered entities must report all breaches of both personally identifiable information (PII) and PHI to the DHA Privacy Office. Reports of such breaches to the DHA Privacy Office must take place within 24 hours of discovery of such breach.

(3) All confirmed cyber-related breaches involving PII and PHI must be reported to the United States Computer Emergency Readiness Team within 1 hour of being confirmed. Non-cyber related breaches should only be reported to the DHA Privacy Office and the Defense Privacy, Civil Liberties, and Transparency Division, as required. Suspected but unconfirmed cyber-related incidents with respect to PHI may be voluntarily submitted to the DHA Privacy Office.

c. Assessments. When a breach is reported, the DoD covered entity or business associate must conduct an initial assessment of the nature of the reported breach, determine whether it qualifies as an HHS breach, what individual notification may be required, and what further mitigation or other response is necessary, in compliance with applicable DoD and HHS requirements and DHA Privacy Office operational guidance. The DHA Privacy Office will review and make the final determination on the subject matter of these initial assessments.

d. Individual Notification. If the initial assessment indicates that individual notification is required, the DoD covered entity or business associate must submit a proposed notification letter to the DHA Privacy Office. The DHA Privacy Office will make the final determination of whether individual notification is required and the contents of the notification letter. For breaches occurring within a DoD covered entity, proposed notification letters must be approved by the Chief, DHA Privacy Office only when the breach is determined to be reportable to HHS. Individual notification letters must include the elements required by HHS in Section 164.404(c)(1) of the HIPAA Breach Rule as set forth in Paragraph 6.2.d.(1).

(1) Individual notification letters must be written in plain language and must include the following elements to the extent possible:

(a) A brief description of what happened, including the date of the breach, if known, and the date of the discovery of the breach.

(b) A description of the types of PHI that were involved in the breach.

(c) Any steps individuals should take to protect themselves from potential harm resulting from the breach.

(d) A brief description of what the DoD covered entity or business associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.

(e) Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, website, or postal address.

(2) Substitute notice is required if insufficient or out-of-date contact information precludes sending individual notification letters. The DoD covered entity or business associate must submit to the DHA Privacy Office a proposed substitute form of notice in accordance with Section 164.404(d)(2) of the HIPAA Breach Rule.

(a) The DHA Privacy Office will make the final determination regarding substitute notice in each case not occurring within a DoD covered entity. However, as with individual notifications, for breaches occurring within a DoD covered entity, proposed substitute notices must be approved by the DHA Privacy Office only when the breach is determined to be reportable to HHS.

(b) The substitute notice must be reasonably calculated to reach the individuals for whom contact information is lacking. If the number of such individuals is fewer than 10, then substitute notice may be provided by an alternative form or written notice, telephone, or other means. If the number of such individuals is 10 or more, then such substitute notice must either be a website posting or media notice (see Paragraph 6.2.e.(2)), plus a toll-free telephone number, as provided in Section 164.404(d)(2)(ii) of the HIPAA Breach Rule.

(3) In any case deemed by the DHA Privacy Office to require urgency because of possible imminent misuse of PHI, the DHA Privacy Office may require notifying individuals by telephone or other means, as appropriate, in addition to other notice provided hereunder.

e. Media Notification. DoD covered entities and business associates, in conjunction with their public affairs office and the DHA Privacy Office, are responsible for establishing a protocol for media notification and website posts for public disclosure of breaches. If the DHA Privacy Office determines that the breach qualifies as an HHS breach, then the DHA Privacy Office must work with the appropriate DoD Component to ensure the proposed announcement complies with the media notification requirements in Sections 164.406 and 164.404(d)(2)(ii)(A) of the HIPAA Breach Rule.

(1) If an HHS breach involves more than 500 residents of a State or jurisdiction, then Section 164.406 of the HIPAA Breach Rule requires notifying prominent media outlets serving the State or jurisdiction.

(2) If it is determined that media notice is required as substitute individual notice under Paragraph 6.2.d.(2), then Section 164.404(d)(2)(ii)(A) of the HIPAA Breach Rule requires conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

f. Reporting to Secretary of HHS. If the DHA Privacy Office determines the breach qualifies as an HHS breach, the DHA Privacy Office must report the breach directly to the Secretary of HHS and provide a copy of such report to the DoD covered entity or business associate.

g. Special Rules.

(1) **Breaches Treated as Discovered.** A breach of PHI will be treated as discovered as of the first day on which the breach is known or suspected. A DoD covered entity or business associate is deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member, employee, or other agent of the DoD covered entity or business associate.

(2) **Law Enforcement Delay.** If a law enforcement official states to a DoD covered entity or business associate that any public notification, such as a web notice, individual notification letter or posting required by this section, would impede a criminal investigation or cause damage to national security, the DoD covered entity, business associate, and DHA Privacy Office must work together to respond to such requests.

(a) If the law enforcement official's request is in writing and states the time for which delay is required, then the notification must be delayed for the time period specified by the official.

(b) If the law enforcement official's request is made orally, the request must be documented, including the identity of the official, and the notification may be delayed no longer than 30 days from the date of the request unless a written statement is obtained during that time.

(3) **Training.** In accordance with Paragraph 7.1.b., DoD covered entities and their business associates must ensure that all workforce members receive training on breach response pursuant to DoD and MHS policy. Additional training must be provided to workforce members who are responsible for carrying out the breach response requirements of this issuance.

(4) **Burden of Proof.** DoD covered entities and their business associates have the burden of demonstrating that all notifications are made as required by this issuance. Documentation to meet this burden of proof must be maintained in accordance with Paragraph 6.2.h.

(5) **Inquiries.** Direct all questions regarding breach response requirements for PHI breaches, to the DHA Privacy Office.

h. Documentation.

(1) In accordance with Paragraph 7.3.d., DoD covered entities and their business associates must ensure that proper documentation is maintained for activities relating to breach reporting, assessment, and notification. The DHA Privacy Office is responsible for documenting decisions on reporting to HHS and maintaining documentation of report submissions to HHS. The DHA Privacy Office report of submissions to HHS must include the elements required by Section 164.408 of the HIPAA Breach Rule and the HHS Website. These elements must therefore be included in reports to the DHA Privacy Office by DoD covered entities and business associates.

(2) Documentation materials may include, for example, internal e-mails, electronic audit log printouts, meeting minutes, and other material that would be needed in the event of a DHA Privacy Office or HHS request for proof of required information, actions, assessments, or decisions. The DoD covered entity or business associate must maintain such documentation materials with respect to every breach, suspected or confirmed, and deliver them to the DHA Privacy Office upon request. Documentation should cover:

(a) Initial discovery, including the date of discovery, the personnel involved in the discovery, and date(s) of the breach, if known.

(b) Copies of initial reports of the breach to the United States Computer Emergency Readiness Team as required by DoD Privacy Program issuances and the reports to the DHA Privacy Office under this issuance (or documentation of any decision that reporting is not required).

(c) The contents and nature of the PHI involved, including the types of identifiers and the likelihood of re-identification.

(d) Internal assessments and associated correspondence within or between the DoD covered entity and business associate, including documentation regarding whether or not unsecured PHI is involved, an HHS breach occurred, and individual notification is required.

(e) All available information about the unauthorized person(s) who used the PHI or to whom the disclosure was made, and whether or not the PHI was actually acquired or viewed, including audit log records and forensic analysis of any computer hardware involved.

(f) Identities of the affected individuals, actions taken to identify those individuals, and when their identities were ascertained.

(g) Documentation of all notification letters, paper or electronic, sent to affected individuals, including their postal or e-mail addresses, and including the dates of mailing or other transmittal.

(h) Documentation of any substitute notifications (including records of calls made), media notices, web postings, and toll-free telephone arrangements.

(i) All data elements needed for the DHA Privacy Office to submit on-time, complete breach reports to HHS using the HHS online reporting form.

(j) Documentation of any assessments and actions taken regarding mitigation of the breach and the extent to which risk to the PHI has been mitigated.



(k) The name and contact information of the person(s) at the DoD covered entity or business associate with whom the DHA Privacy Office can seek further information regarding the breach.

6.3. BREACH RISK ANALYSIS TEMPLATE.

a. Risk analysis. Figure 1 assists DoD covered entities in providing risk analysis documentation in connection with a breach involving PHI.

b. Updates to template. This template is current as of the date of this issuance and is subject to change by the DHA Privacy Office without modifying or reissuing this issuance. The DHA Privacy Office will communicate to DoD covered entities and business associates any changes to the template to assure that they are using the current template in connection with performing the risk analysis.

Figure 1: DHA Privacy Office Breach Risk Analysis Template

 <p>DHA Defense Health Agency</p>	<h2 style="margin: 0;">Breach Risk Analysis Template</h2> <h1 style="margin: 10px 0 0 0; color: red;">SAMPLE</h1>	
Section 1.		
DoD Covered Entity Involved Sample Military Treatment Facility (MTF)	Date of Discovery 10/16/18	Tracking # 2018-00-123
Total Number of Potentially Impacted Individuals		1
Section 2.		
<p>1) Is the information unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Department of Health and Human Services (refer to Section 13402(h)(2) of HITECH Act)?</p> <p style="margin-left: 20px;">No</p> <p><i>If Yes, then STOP here. No breach has occurred that requires notification. If No, then proceed to next question.</i></p>		
<p>2) Is there evidence to indicate that the information was NOT viewed or accessed by an unintended/unauthorized party?</p> <p style="margin-left: 20px;">Yes</p> <p><i>If Yes, then no breach has occurred that requires notification. If No, then proceed to Section 3.</i></p>		
Section 3.		
<p>Does one of the following exceptions apply?</p> <p style="margin-left: 20px;">No</p> <p><i>If Yes, select the appropriate exception below.</i></p> <ul style="list-style-type: none"> a. Good faith, unintentional acquisition, access or use of PHI, within the scope of duty, by an employee/workforce member of a DoD covered entity. b. Inadvertent disclosure to another person authorized to handle PHI within the DoD covered entity. c. Recipient could not reasonably have retained the data. 		
Section 4. [Breach Risk Analysis Template - continued]		
<p>Final Determination</p> <p>The medical records for one individual could not be located following an extensive search. A timely notification letter was provided to the individual. Based on our assessment of the incident, the DHA Privacy Office has determined this breach does meet the criteria of being reportable to HHS.</p>		

SECTION 7: ADMINISTRATIVE AND TRANSITION PROVISIONS

7.1. PERSONNEL REQUIREMENTS.

a. Personnel Designations.

(1) Standard: Personnel Designations.

(a) A DoD covered entity, including an MTF, must designate in writing a HIPAA privacy officer who is responsible for the development and implementation of the policies and procedures of the entity pertaining to the protection of health information under this issuance.

(b) A DoD covered entity, including an MTF, must designate a HIPAA privacy officer that is responsible for receiving complaints under Paragraph 7.2. and who is able to provide further information about matters covered by the NoPP required by Paragraph 5.1.

(2) **Implementation Specification: Personnel Designations.** A DoD covered entity must document the personnel designations in Paragraph 7.1.a.(1) as required by Paragraph 7.3.d.

b. Training.

(1) **Standard: Training.** A DoD covered entity must train all members of its workforce on the policies and procedures regarding PHI required by Paragraph 7.3.c., as necessary and appropriate for the members of the workforce to carry out their function within the DoD covered entity.

(2) **Implementation Specifications: Training.**

(a) A DoD covered entity must provide training that meets the requirements of Paragraph 7.1.b.(1). Training must be provided:

1. To each member of the DoD covered entity's workforce no later than the compliance date for the DoD covered entity.

2. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the DoD covered entity's workforce. The training must also include information about the local policies and procedures which pertain to the protection of health information.

3. To all workforce members, annually, as a refresher.

4. To each member of the workforce whose functions are affected by a material change in policies or procedures pertaining to the protection of health information. The training must occur within a reasonable period of time after the material change becomes effective in accordance with Paragraph 7.3.c.

(b) Contracted health care providers and other contracted personnel providing services in an MTF must be included in the training described in Paragraph 7.1.b.(2).

(c) Reserve Component personnel who are assigned to or provide operational support to an MTF as a result of mobilization or who provide support during a drill or annual training period are considered a member of the MTF workforce and must complete the training outlined in Paragraph 7.1.b.

(d) A DoD covered entity must document that the training as described in Paragraph 7.1.b.(2) has been provided, as required by Paragraph 7.3.d. The DoD covered entity must ensure maintenance of a complete, accurate, and up to date record of the HIPAA training status of all DoD covered entity personnel and workforce members to ensure compliance with this issuance. A DoD covered entity must ensure that policies and procedures of the DoD covered entity regarding the in-processing of new workforce members and the out-processing of departing or terminated workforce members include the DoD covered entity's HIPAA privacy officer.

(e) Contractor workforce members who access PHI in performing their functions must receive appropriate training. Their training may be provided by the contractor, a DoD covered entity, or both, in accordance with contract terms and DHA guidance. Contractors must ensure that workforce members of subcontractors receive appropriate training.

c. Sanctions.

(1) Standard: Sanctions.

(a) A DoD covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the DoD covered entity or the requirements of this issuance. The sanctions must reasonably relate to the severity and nature of the failure or misconduct.

1. For Service members, this may include action under the UCMJ, administrative, or other appropriate sanctions.

2. For civilian employees, sanctions must be applied consistent with the provisions of Chapter 75 of Title 5, U.S.C.

3. For contractor personnel subject to this paragraph, sanctions may include actions permissible under applicable procurement regulations.

(b) This standard does not apply to a member of the DoD covered entity's workforce with respect to actions that are covered by and that meet the conditions of Paragraph 4.5.f. or Paragraph 7.2.b.(2).

(2) Implementation Specification: Documentation. As required by Paragraph 7.3.d., a DoD covered entity must document the sanctions that are applied, if any.

7.2. PROTECTIONS FOR INDIVIDUALS AND OTHERS.

a. Complaints.

(1) **Standard: Complaints to the DoD Covered Entity.** A DoD covered entity, including an MTF, must provide a process for individuals to make complaints concerning the DoD covered entity's policies and procedures required by this issuance or its compliance with such policies and procedures or the requirements of this issuance.

(2) **Implementation Specification: Processing of Complaints.** Individuals may file a HIPAA complaint directly with the involved DoD covered entity, the DHA Privacy Office, or HHS. When an individual files a HIPAA complaint directly with a DoD covered entity, that entity must direct the complaint to its HIPAA privacy officer for action. DHA will ensure instructions on how to file a HIPAA complaint are made available to individuals. The HHS HIPAA complaint form is available on the HHS Website.

(a) HIPAA complaints received by a DoD covered entity directly from an individual are not required to be provided to or coordinated with the DHA Privacy Office.

(b) Upon receipt of a HIPAA complaint from HHS, a DoD covered entity's HIPAA privacy officer must forward the complaint to the DHA Privacy Office within 5 days of receipt, along with any relevant information and documentation available to that HIPAA privacy officer pertaining to the complaint's allegations. The DHA Privacy Office is the designated liaison office for handling all HIPAA complaints against DoD covered entities submitted to HHS.

(c) Following receipt of a HIPAA complaint from an individual or HHS, the DHA Privacy Office will, in accordance with DHA Privacy Office policies and procedures:

1. Provide a copy of the HIPAA complaint to the appropriate HIPAA privacy officer.

2. Initiate, coordinate, and monitor the investigation process with the appropriate HIPAA privacy officer.

3. Assign the appropriate investigation suspense date(s) and provide instructions as to how to request a suspense extension.

4. Provide, or forward from HHS, a list of documentation required to complete the resolution of the HIPAA complaint.

(d) After completing its investigation of a HIPAA complaint received from an individual or HHS, a DoD covered entity must forward its investigation report to the local HIPAA privacy officer, who must forward the report to the DHA Privacy Office for review. Once the investigation response is determined to be complete, the DHA Privacy Office must provide the HIPAA complaint resolution response to HHS or the individual.

(e) The DHA Privacy Office must coordinate all communications regarding a HIPAA complaint and investigation.

(3) **Implementation Specification: Documentation of Complaints.** As required by Paragraph 7.3.d., a covered entity must document all complaints received, and their disposition, if any.

b. Standard: Refraining from Intimidating or Retaliatory Acts. A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(1) **Individuals.** Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this issuance, including the filing of a complaint.

(2) **Individuals and Others.** Any individual or other person for:

(a) Filing a complaint with HHS under Subpart C of Part 160 of Title 45, CFR.

(b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Subtitle A, Subchapter C of Title 45, CFR.

(c) Opposing any act or practice made unlawful by this issuance, if the individual or person has a good faith belief the practice is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of this issuance.

c. Standard: Waiver of Rights. A DoD covered entity may not require individuals to waive their rights under this issuance as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

7.3. OTHER COVERED ENTITY REQUIREMENTS.

a. Safeguards.

(1) **Standard: Safeguards.** A DoD covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

(2) **Implementation Specification: Safeguards.**

(a) A DoD covered entity must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements of this issuance.

(b) A DoD covered entity must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

b. Standard: Mitigation. A DoD covered entity must mitigate, when practicable, any harmful effect that is known to the DoD covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of this issuance by the DoD covered entity or its business associate.

c. Policies and Procedures.

(1) **Standard: Policies and Procedures.** A DoD covered entity must implement policies and procedures on PHI that are designed to comply with the standards, implementation specifications, or other requirements of this issuance. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to PHI undertaken by the DoD covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this issuance.

(2) **Standard: Changes to Policies or Procedures.**

(a) Changes to privacy practices may not become effective until all required changes to the MHS NoPP are effective. Changes to privacy practices may be retroactively effective for PHI that was created or received before the effective date of the MHS NoPP revision.

(b) A DoD covered entity may make any other changes to policies and procedures at any time, if the changes are documented and implemented in accordance with Paragraph 7.3.c.(5).

(3) **Implementation Specification: Changes in Law.**

(a) Whenever there is a change in law that a DoD covered entity determines as possibly necessitating a material change to the DoD covered entity's policies or procedures, the DoD covered entity must promptly document the proposed changes and provide notification to the DHA Privacy Office, including the DoD covered entity's recommendations for changes to the MHS NoPP.

(b) If the DHA Privacy Office determines that the change in law materially affects the content of the NoPP required by Paragraph 5.1., the DHA Privacy Office will undertake efforts to make the appropriate revisions to the NoPP in accordance with Paragraph 5.1.b.(2).

(c) Nothing in this paragraph may be used by a DoD covered entity to excuse a failure to comply with the law. No changes will be made to the NoPP without the prior written approval of the DHA Privacy Office.

(4) **Implementation Specifications: Changes to Privacy Practices Stated in NoPP.**

(a) To implement a change as provided by Paragraph 7.3.c.(2)(a), a DoD covered entity must:

1. Ensure that the policy or procedure, as revised to reflect a change in the DoD covered entity's privacy practice as stated in its NoPP, complies with the standards, requirements, and implementation specifications of this issuance.

2. Document the policy or procedure, as revised, as required by Paragraph 7.3.d.

3. Revise the NoPP as required by Paragraph 5.1.b.(2) to state the changed practice and submit the changed practice and revised NoPP to the DHA Privacy Office for

approval. The DoD covered entity may not implement a change to a policy or procedure prior to the effective date of the revised NoPP.

(5) **Implementation Specification: Changes to Other Policies or Procedures.** A DoD covered entity may change, at any time, a policy or procedure that does not materially affect the content of the NoPP required by Paragraph 5.1., if:

(a) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this issuance.

(b) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by Paragraph 7.3.d.

d. Documentation.

(1) **Standard: Documentation.** A DoD covered entity must:

(a) Maintain the policies and procedures provided for in Paragraph 7.3.c. in written or electronic form.

(b) If written communication is required by this issuance, maintain communication, or an electronic copy, as documentation.

(c) If documented action, activity, or designation is required by this issuance, maintain a written or electronic record of such action, activity, or designation.

(2) **Implementation Specification: Retention Period.** A DoD covered entity must retain the documentation required by Paragraph 7.3.d.(1) for 6 years from the date of its creation or the date when it last was in effect, whichever is later, unless a longer period is specified by the National Archives and Records Administration or by DoD or DoD Component records management regulations and guidance applicable to it. This retention period only applies to the documentation required by this issuance and the HIPAA Privacy Rule. This requirement does not apply to records containing PHI for which medical record retention periods longer than 6 years are imposed by other laws, regulations, and DoD Component issuances.

7.4. COMPLIANCE DATES AND TRANSITION PROVISIONS.

a. Standard: Effect of Prior Authorizations. Notwithstanding Paragraph 4.2. and Paragraph 4.4.i., a DoD covered entity may use or disclose PHI, consistent with this paragraph, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of PHI, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB, or waiver of authorization in accordance with Paragraph 4.4.i.(a)(1).

(1) **Implementation Specification: Effect of Prior Authorization for Purposes Other Than Research.** Notwithstanding any provisions in Paragraph 4.2., a DoD covered entity may use or disclose PHI that it created or received prior to the applicable compliance date of this issuance

pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this issuance, if the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with Paragraph 5.2.a.

(2) Implementation Specification: Effect of Prior Permission for Research.

Notwithstanding any provisions in Paragraph 4.2. and Paragraph 4.4.i., a DoD covered entity may, to the extent allowed by one of the following permissions, use or disclose, for a research study, PHI that it created or received either before or after the applicable compliance date of this issuance, if there is no agreed-to restriction in accordance with Paragraph 5.2.a.(1)(a) and the DoD covered entity has obtained, prior to the applicable compliance date, either:

(a) An authorization or other express legal permission from an individual to use or disclose PHI for the research;

(b) The informed consent of the individual to participate in the research;

(c) A waiver, by an IRB, of informed consent for the research, in accordance with the Common Rule, Section 219.116(d) of Title 32, CFR (or comparable regulation of another federal agency), provided that a DoD covered entity must obtain authorization in accordance with Paragraph 4.2. if, after the compliance date, informed consent is sought from an individual participating in the research; or

(d) A waiver of authorization in accordance with Paragraph 4.4.i.(a)(1).

b. Business Associate Arrangements and Data Use Agreements. Sections 164.534(d)-(f) of Title 45, CFR, details transitional provisions relating to business associate agreements and data use agreements in effect as of January 25, 2013. Corresponding provisions are not included here, because all such agreements are now renewed, amended, or terminated.

GLOSSARY

G.1. ACRONYMS.

ASD(HA)	Assistant Secretary of Defense for Health Affairs
CFR	Code of Federal Regulations
DHA	Defense Health Agency
DHS	Department of Homeland Security
DoDD	DoD Directive
DoDI	DoD Instruction
FDA	Food and Drug Administration
FOIA	Freedom of Information Act
GC DoD	General Counsel of the Department of Defense
HHS	Department of Health and Human Services
HITECH	Health Information Technology for Economic and Clinical Health
HIPAA	Health Insurance Portability and Accountability Act
IRB	Institutional Review Board
MHS	Military Health System
MTF	military treatment facility
NoPP	Notice of Privacy Practices
PHI	protected health information
PII	personally identifiable information
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code
VA	Department of Veterans Affairs

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance. The Glossary definitions assign HIPAA-specific meanings to the following common terms: use, disclose/disclosure, individual, payment, and required by law.

breach or DoD breach. As defined in OMB Memorandum M-17-12, the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses personally identifiable

information; or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

business associate. Except as provided below, a business associate, with respect to a DoD covered entity, is:

A person who, on behalf of such DoD covered entity or of an organized health care arrangement in which the DoD covered entity participates, but other than in the capacity of a member of the workforce of such DoD covered entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by this issuance, or performs, or assists in the performance of a function or activity involving the use or disclosure of PHI or other function or activity regulated by this issuance; or

A person who provides, other than in the capacity of a member of the workforce of such DoD covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such DoD covered entity, or to or for an organized health care arrangement in which the DoD covered entity participates, where the provision of the service involves the disclosure of PHI from such DoD covered entity or arrangement, or from another business associate of such DoD covered entity or arrangement, to the person.

In certain circumstances, a DoD or other covered entity performing HIPAA-covered functions on behalf of another covered entity. This circumstance occurs only when the first covered entity is not acting as either a health plan or a provider covered entity in its dealings with the other covered entity. For example, some of the managed care support contractors act as health plan covered entities (insurers) in their commercial business but act as administrative service providers (and thus as business associates) with respect to the TRICARE health plan.

Business associate includes:

A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a DoD covered entity and that requires access on a routine basis to such PHI.

A person that offers a personal health record to one or more individuals on behalf of a DoD covered entity.

A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Business associate does not include:

A health care provider, with respect to disclosures by a DoD covered entity to the health care provider concerning the treatment of the individual.

A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

A DoD covered entity participating in an organized health care arrangement that performs a function or activity as described by the second paragraph of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in the third paragraph of this definition to or for such organized health care arrangement by virtue of such activities or services.

correctional institution. Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody include juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. The term “correctional institution” includes military confinement facilities, but does not include internment facilities for enemy prisoners of war, retained personnel, civilian detainees, and other detainees provided under the provisions of DoDD 2310.01E.

covered entity. A health plan or a health care provider who transmits any health information in electronic form in connection with a standard transaction covered by this issuance. To the extent this issuance prescribes duties to be performed by covered entities, such duties apply only to DoD covered entities.

covered functions. Those functions of a covered entity, the performance of which makes the entity a health plan or health care provider.

data aggregation. With respect to PHI created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such PHI by the business associate with the PHI received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

de-identification of PHI. Health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

designated record set. For purposes of this definition, the term “record” means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

A group of records maintained by or for a covered entity that is:

The medical records and billing records about individuals maintained by or for a covered health care provider.

The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

Used, in whole or in part, by or for the covered entity to make decisions about individuals.

DHA publication. One of the four types of publications published by the DHA taking the form of DHA-Procedural Instructions, DHA-Procedures Manuals, DHA-Interim Procedures Memorandums, and DHA-Administrative Instructions. DHA publications do not establish policy, they provide procedural guidance to implement policy from DoD issuances, federal law, or U.S.C.

direct treatment relationship. A treatment relationship between an individual and a health care provider that involves face-to-face interaction between the individual and health care provider or that otherwise does not involve an intermediary.

disclose or disclosing. To release, transfer, provide access to, or otherwise divulge PHI outside the entity holding the information

disclosure. The release, transfer, provision of access to, or other divulging in any manner of PHI outside the entity holding the information.

DoD breach response requirements. The breach response provisions in the DoD Privacy Program issuances and related breach response guidance from the Office of Management and Budget and DHS.

DoD Component. Defined in DoDI 5025.01.

DoD covered entity. In the case of a health plan administered by DoD, the DoD covered entity is the DoD Component or subcomponent that functions as the administrator of the health plan. Not all health care providers affiliated with the Military Services are DoD covered entities. Examples of providers that are not DoD covered entities are providers associated with Military Entrance Processing Stations or DoD Medical Examination Review Board and Reserve components practicing outside the authority of MTFs who do not engage in electronic transactions covered by this issuance (see the definition of standard transactions).

DoD cybersecurity requirements. Current DoD issuances and other federal law relating to electronic data security and protection of DoD information systems, as identified by DHA Privacy Office guidance. These DoD issuances include, but are not limited to, DoDI 8500.01, DoDI 8510.01, and DoDI 8580.02.

DoD identification number. Defined in DoDI 1000.30.

DoD issuance. Also called “issuance” in this manual. One of the five types of issuances published by the DoD that establishes or implements DoD policy, designates authority, assigns responsibilities, or provides procedures. Issuances apply to more than one DoD Component and include DoD directives, DoD instructions, DoD manuals, DoD Directive-type Memorandums, and DoD administrative instructions.

DoD Privacy Program issuances. Current DoD issuances implementing within DoD the Privacy Act and certain privacy-related authorities, as identified by DHA Privacy Office guidance.

eHealth Exchange. A group of federal agencies and non-federal organizations that have by agreement established an interoperable health information exchange to facilitate permissible uses and disclosures of PHI. Participating organizations mutually agree to support a common set of standards and specifications that enable the establishment of a secure, trusted, and interoperable connection among all participating organizations.

electronic media. Electronic storage media on which data is or may be recorded electronically, including; hard drives, any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card, or transmission media used to exchange information already in electronic storage media. Transmission media include the Internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties) or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

employment records. Records that include health information and are maintained by a component of the DoD or other entity subject to this issuance; are about an individual who is (or seeks or sought to become) a member of the Uniformed Services, employee of the United States Government, employee of a DoD contractor, or person with a comparable relationship to the DoD; and are not maintained in connection with carrying out any covered function under this issuance.

federal agency. Each authority of the U.S. Government, whether or not it is within or subject to review by another agency.

government agency. Federal agency or any unit of State or local government.

health care. Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body.

Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

health care operations. Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, if obtaining general knowledge is not the

primary purpose of any studies resulting from such activities; patient safety activities as defined in Section 3.20 of Title 42, CFR; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

Enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance).

Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection, and compliance programs.

Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment, or coverage policies.

Business management and general administrative activities of the entity including, but not limited to:

Management activities relating to implementation of and compliance with the requirements of this issuance.

Customer service, if PHI is not disclosed except as otherwise permitted by this issuance.

Resolution of internal grievances.

The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity.

Creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

health care provider. Any MTF, including garrison clinics and such facilities in a military operational unit, ship, or aircraft, and any other person or organization outside of such facilities' workforce who furnishes, bills, or is paid for health care in the normal course of business. This term includes occupational health clinics for civilian employees or contractor personnel.

health information. Any information, including genetic information, in any form or medium, that:

Is created or received by a health care provider, health plan, public health authority, employer, life insurer, or school or university.

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

health oversight agency. An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Any DoD Component authorized under applicable DoD issuances or other applicable publications to oversee the MHS, including with respect to matters of quality of care, risk management, program integrity, financial management, standards of conduct, or the effectiveness of the MHS in carrying out its mission.

health plan. Any DoD program that provides or pays the cost of health care, unless exempted under this definition of health plan.

The following components of the TRICARE Program are a health plan under this issuance:

The program that provides health care under the authority of the Department of the Army to members of the Uniformed Services. (Administrator: Surgeon General of the Army.)

The program that provides health care under the authority of the Department of the Navy to members of the Uniformed Services. (Administrator: Surgeon General of the Navy.)

The program that provides health care under the authority of the Department of the Air Force to members of the Uniformed Services. (Administrator: Surgeon General of the Air Force.)

The Supplemental Care Program under Section 1074c of Title 10, U.S.C., and Section 199.16 of Title 32, CFR, for members of the Army, Navy, Marine Corps, and Air Force who receive health care services from providers other than providers of the DoD. (Administrators: Surgeon General of the Army for members of the Army; Surgeon General of the Navy for members of the Navy and Marine Corps; Surgeon General of the Air Force for members of the Air Force.)

The TRICARE Prime and TRICARE Select (including plans previously known as TRICARE Extra, and TRICARE Standard) health care options offered under Section 199.17 of Title 32, CFR. (Administrator: DHA.)

The health care program for the uniformed services under Chapter 55 of Title 10, U.S.C. (Administrator: DHA.)

The following are also included as health plans:

The TRICARE Dental Program under Section 1076a of Title 10, U.S.C. (Administrator: DHA.)

The TRICARE Retiree Dental Program under Section 1076c of Title 10, U.S.C. (Administrator: DHA.)

The Continued Health Care Benefit Program under Section 1078a of Title 10, U.S.C. (Administrator: DHA.)

The Designated Provider Program under Section 1073 of Title 10, U.S.C. (Administrator: DHA.)

Programs conducted as demonstration projects under Section 1092 of Title 10, U.S.C. to the extent not otherwise included under a health plan.

The pharmacy benefits program offered under Section 199.21 of Title 32, CFR.

The TRICARE Reserve Select program offered under Section 199.24 of Title 32, CFR.

The TRICARE Retired Reserve program offered under Section 199.25 of Title 32, CFR.

Health plan excludes the following DoD programs:

Although part of the TRICARE Program, the programs that provide health care in medical and dental treatment facilities of the Departments of the Army, Navy, and Air Force to beneficiaries other than members of the Military Services are excluded by the HIPAA Rules from the definition of health plan.

The Women, Infants, and Children Program.

Occupational health clinics for civilian employees or contractor personnel.

Any other policy, plan, or program to the extent that it provides, or pays for the cost of workers' compensation benefits or insurance coverage such as liability, accident, automobile, disability, or similar coverage.

Any other program whose principal purpose is other than providing, or paying the cost of, health care.

Any other program (other than one identified as specifically being a health plan) whose principal activity is the direct provision of health care to persons.

Any other program whose principal activity is the making of grants to fund the direct provision of health care to persons.

HHS breach. A breach as defined in Section 164.402 of the HIPAA Breach Rule. The text of that HHS definition states:

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part [i.e. the HIPAA Privacy Rule] which compromises the security or privacy of the PHI.

HHS breach excludes:

Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a DoD covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

Any inadvertent disclosure by a person who is authorized to access PHI at a DoD covered entity or business associate to another person authorized to access PHI at the same DoD covered entity or business associate, or organized health care arrangement in which the DoD covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted the HIPAA Privacy Rule.

A disclosure of PHI where a DoD covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except as provided in this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under this issuance is presumed to be a breach unless the DoD covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

The unauthorized person who used the PHI or to whom the disclosure was made;

Whether the PHI was actually acquired or viewed; and

The extent to which the risk to the PHI has been mitigated.

HIPAA complaint. A written statement submitted to a DoD covered entity's HIPAA privacy officer or to the HHS Office for Civil Rights alleging that the DoD covered entity has violated an individual's health information privacy rights or committed a violation of the HIPAA Privacy or Security Rule provisions.

HIPAA privacy officer. The member of the workforce of a DoD covered entity or DoD Component who is the designated point of contact for the DoD covered entity or component for handling HIPAA privacy complaints. Such workforce member may be a member of a Military Service, a DoD civilian employee, or a contractor of the DoD covered entity or component. As stated in Paragraph 2.2.c(1), a DoD covered entity’s HIPAA privacy officer may also be the designated HIPAA security officer for that DoD covered entity as provided in DoDI 8580.02.

HIPAA Rules. The regulations issued by HHS pursuant to its authority to issue regulations on health information privacy, as provided by Section 264(c) of HIPAA. The HIPAA Rules, as amended by the Omnibus Final Rule, include the HIPAA Privacy Rule, the HIPAA Breach Rule, the HIPAA Security Rule, and the HIPAA Enforcement Rule.

The term HIPAA Rules does **not** include the HIPAA “Administrative Requirements” rules at Part 162 of Title 45, CFR, which relate to identifiers, standard transactions, and code sets.

HITECH Act. Title XIII and Title IV of Division B of Public Law 111-5 “may be cited as the ‘Health Information Technology for Economic and Clinical Health Act’ or the ‘HITECH Act,’” as provided in Section 13001(a) of Public Law 111-5. As used in this issuance, the term HITECH Act refers to Title XIII, Subtitle D of Public Law 111-5, requiring changes to the HIPAA Privacy, Security and Enforcement Rules, and providing for a new HIPAA Breach Rule. HHS implemented these HITECH Act changes by issuing regulations known as the Omnibus Final Rule.

implementation specification. Specific requirements or instructions for implementing a standard.

individual. The person who is the subject of PHI. Under certain circumstances, such as those in Paragraph 4.5.g., rights of an individual under this issuance may be exercised by a personal representative.

individually identifiable health information. Information that is a subset of health information, including demographic information collected from an individual, and:

Is created or received by a health care provider, health plan, or employer; and

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

in loco parentis. In the place of a parent.

jurisdiction. A geographic area smaller than a State, such as a county, city, or town.

law enforcement official. An officer or employee of any agency or authority of the United States (including an officer, employee, or designated member of a Military Service or other DoD Component), a State, a territory, a political subdivision of a State or territory, or an Indian tribe,

who is empowered by law to: investigate or conduct an official inquiry into a potential violation of law, including the UCMJ, or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law, including violations of the UCMJ. Such persons include, but are not limited to those persons in the Military Services.

marketing. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing includes an arrangement between a DoD covered entity and any other entity whereby the DoD covered entity disclosed PHI to the other entity, in exchange for direct or indirect payment, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service. Marketing does not include a communication made:

To inform an individual who is a member of a Uniformed Service or a covered beneficiary of the MHS of benefits, services, coverages, limitations, costs, procedures, rights, obligations, options, and other information concerning the MHS as established by law and applicable regulations.

To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any payment received by the DoD covered entity in exchange for making the communication is reasonably related to the DoD covered entity's cost of making the communication.

For the following treatment and health care operations purposes, except where the DoD covered entity receives payment in exchange for making the communication:

For treatment of an individual by a health care provider including case management or care coordination of the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the DoD covered entity making the communication, including communication about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

MHS. All DoD health plans and all DoD health care providers that are, in the case of institutional providers, organized under 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.

MHS non-active duty health care recipient. Patients (excluding active duty or Reserve

Component Service members eligible to receive care) who are eligible to receive health care through TRICARE or were treated in an MHS facility.

MTF. Established for the purpose of furnishing medical care, dental care, or both to eligible individuals.

NoPP. The notice of the MHS's practices and procedures with respect to safeguarding the confidentiality, integrity, and availability of an individual's PHI, and the rights of individuals with respect to their PHI as provided for in Paragraph 5.1 of this issuance.

Omnibus Final Rule. The "Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules," Volume 78, Federal Register, January 25, 2013.

opt out. The choice by a beneficiary (excluding active duty or Reserve Component Service members eligible to receive care) to not permit sharing of his or her health data by MHS with non-MHS eHealth Exchange partners.

organized health care arrangement. An organized system of health care in which participating covered entities 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 Coast Guard are a single organized health care arrangement.

other applicable publication.

A DHA publication.

The Manual for Courts-Martial or other issuance of the President applicable to the Armed Forces.

A Military Department or Military Service regulation or issuance of the Chairman of the Joint Chiefs of Staff to the extent the DHA Privacy Office determines is consistent with the policies and procedures of this manual.

payment. Except as prohibited by Paragraph 4.4.j:

The activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Payment activities relate to the individual to whom health care is provided and include, but are not limited to:

Determinations of eligibility or coverage including coordination of benefits or the determination of cost sharing amounts, and adjudication or subrogation of health benefit claims.

Risk adjusting amounts due based on enrollee health status and demographic characteristics.

Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing.

Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.

Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services.

Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address; date of birth; social security number; payment history; account number; and name and address of the health care provider or health plan.

PHI. Individually identifiable health information that 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 which has been de-identified in accordance with Paragraph 4.5.a is not PHI. PHI is a subset of PII, with respect to living persons.

PII. Defined in OMB Circular No. A-130.

Privacy Act. A federal statute, codified in Section 552a of Title 5, U.S.C., that, among other things, protects the confidentiality of federal records maintained on individuals. In contrast to HIPAA, applicability of the Privacy Act is limited to the federal government.

psychotherapy notes. Notes recorded, in any medium, by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private, group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

public health authority. An agency or authority of the United States, a State, territory, political subdivision of State or territory, Indian tribe, or person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. The term "public health authority" includes any DoD Component authorized under applicable DoD issuance or other applicable publication to carry out public health activities, including medical surveillance activities under DoDD 6490.02E.

required by law. A mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.

Includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Also includes any mandate contained in a DoD issuance or other applicable publication that requires a DoD covered entity (or other person functioning under the authority of a DoD covered entity) to make a use or disclosure and is enforceable in a court of law. The attribute of being enforceable in a court of law means that in a court or court-martial proceeding, a person required by the mandate to comply would be held to have a legal duty to comply or, in the case of non-compliance, to have had a legal duty to have complied. Required by law also includes any DoD issuance or other applicable publication requiring the production of information necessary to establish eligibility for reimbursement or coverage under Civil Health and Medical Program of the Uniformed Services/TRICARE.

research. A systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary of HHS. The Secretary of HHS or any other officer or employee of HHS that has been delegated relevant authority.

standard. A rule, condition, or requirement with respect to the privacy or breach of protected health information.

standard transactions. Transmission in electronic form as prescribed by the Secretary of HHS between two or more parties to carry out financial or administrative activities relating to health care provided to a patient.

State. One of the following:

For a health plan established or regulated by federal law, State is defined in the applicable section of the U.S.C. for such health plan.

For all other purposes, State is defined as any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

subcontractor. A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

treatment. The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a

health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

underwriting purposes. With respect to a health plan, includes:

Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program).

The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program).

The application of any pre-existing condition exclusion under the plan, coverage, or policy.

Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

unsecured PHI. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS in guidance issued under Section 13402(h)(2) of Public Law 111-5.

use. With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Virtual Lifetime Electronic Record Health Information Exchange. A set of programs that manages the electronic exchange of beneficiary health information among VA, DoD, other federal agencies, and private partners.

workforce. Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a DoD covered entity or business associate is under the direct control of the DoD covered entity or business associate whether or not they are paid by the DoD covered entity or business associate.

REFERENCES

- Code of Federal Regulations, Title 29, Parts 1904 - 1928 (also known as the “Occupational Safety and Health Administration Regulations”)
- Code of Federal Regulations, Title 30, Parts 50 - 90 (also known as the “Mine Safety and Health Administration Regulations”)
- Code of Federal Regulations, Title 32
- Code of Federal Regulations, Title 42
- Code of Federal Regulations, Title 45
- DoD Directive 1308.1, “DoD Physical Fitness and Body Fat Program,” June 30, 2004
- DoD Directive 2310.01E, “DoD Detainee Program,” August 19, 2014
- DoD Directive 5124.02, “Under Secretary of Defense for Personnel and Readiness (USD(P&R)),” June 23, 2008
- DoD Directive 5136.01, “Assistant Secretary of Defense for Health Affairs (ASD(HA)),” September 30, 2013, as amended
- DoD Directive 5136.13, “Defense Health Agency (DHA),” September 30, 2013
- DoD Directive 5400.11, “DoD Privacy Program,” October 29, 2014
- DoD Directive 6490.02E, “Comprehensive Health Surveillance,” February 8, 2012, as amended
- DoD Instruction 1000.30, “Reduction of Social Security Number (SSN) Use Within DoD,” August 1, 2012
- DoD Instruction 1010.01, “Military Personnel Drug Abuse Testing Program (MPDATP),” September 13, 2012
- DoD Instruction 1010.09, “DoD Civilian Employee Drug-Free Workplace Program,” June 22, 2012
- DoD Instruction 1332.18, “Disability Evaluation System (DES),” August 5, 2014, as amended
- DoD Instruction 3216.02, “Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research,” November 8, 2011
- DoD Instruction 5025.01, “DoD Issuances Program,” August 1, 2016, as amended
- DoD Instruction 5025.13, “DoD Plain Language Program,” April 11, 2013, as amended
- DoD Instruction 5210.42, “Nuclear Weapons Personnel Reliability Assurance,” April 27, 2016
- DoD Instruction 6025.13, “Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS),” February 17, 2011, as amended
- DoD Instruction 6025.18, “Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs,” March 13, 2019
- DoD Instruction 6400.06, “Domestic Abuse Involving DoD Military and Certain Affiliated Personnel,” August 21, 2007, as amended
- DoD Instruction 6490.08, “Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members,” August 17, 2011
- DoD Instruction 6495.02, “Sexual Assault Prevention and Response (SAPR) Program Procedures,” March 28, 2013, as amended
- DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014

DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014, as amended

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

DoD Manual 5400.07, “DoD Freedom of Information Act (FOIA) Program,” January 25, 2017

DoD Manual 8910.01, Volume 1, “DoD Information Collections Manual: Procedures for DoD Public Information Collections,” June 30, 2014, as amended

DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007

Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as amended

Executive Order 13181, “To Protect the Privacy of Protected Health Information in Oversight Investigations,” December 20, 2000

Joint Task Force National Capital Region Medical Directive 5100.01, “The Joint Pathology Center Charter,” November 22, 2011

OMB Circular A-130, “Managing Information as a Strategic Resource,” July 28, 2016

OMB Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information,” January 3, 2017

Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996,” August 21, 1996 (also known as “HIPAA”)

Public Law 111-5, “The American Recovery and Reinvestment Act of 2009,” February 17, 2009

Public Law 111-274, “The Plain Writing Act of 2010,” October 13, 2010

Public Law 113-66, “National Defense Authorization Act for Fiscal Year 2014,” December 26, 2013

United States Code, Title 5

United States Code, Title 10

United States Code, Title 18

United States Code, Title 22 Section 2709(a)(3), as amended

United States Code, Title 28, Sections 2671 - 2680 (also known as the “Federal Tort Claims Act,” as amended)

United States Code, Title 42, as amended

United States Code, Title 50, Section 401 (also known as the “National Security Act,” as amended)