Defense Health Agency

# ADMINISTRATIVE INSTRUCTION

DEC - 2 2014 **NUMBER 75**
[DATE SIGNED]

Privacy Office

SUBJECT: Health Insurance Portability and Accountability Act (HIPAA) Core Tenets Procedures

References: Enclosure 1

1. PURPOSE. This Defense Health Agency Administrative Instruction (DHA-AI), based on the authority of References (a) and (b), and in accordance with the formatting of Reference (c), establishes responsibilities and procedures in accordance with privacy and security requirements outlined in References (d) through (g), and any successor references, as applicable, and details the core tenets of DHA's implementation of the HIPAA Privacy, Security, and Breach Notification Rules for the use, disclosure, and safeguarding of protected health information (PHI).

2. APPLICABILITY. This AI applies to all DHA personnel, to include: assigned or attached Service members, federal civilians, contractors, and other personnel assigned temporary or permanent duties at DHA to include regional and field activities (remote locations).

3. POLICY. It is DHA's policy in accordance with References (d) and (e) that:

a. DHA must ensure the confidentiality, integrity, and availability of all PHI the organization creates, receives, maintains, or transmits, and protect against any reasonably anticipated threats or hazards to the privacy and security of such information.

b. Confidentiality includes protection against any reasonably anticipated uses or disclosures of PHI that are not permitted or required by References (d) and (f), as well as ensuring that permitted uses and disclosures are in accordance with Reference (d) and (f).

4. RESPONSIBILITIES.

a. Director, DHA. The Director, DHA shall:

(1) Exercise oversight over DHA to ensure compliance with this AI.

(2) Oversee coordination of implementation of this AI between the DHA Privacy Office and the DHA Health Information Technology Directorate.

(3) Delegate authority to the DHA Privacy Office to develop and update supporting guidance under this AI as necessary.

b. Chief, DHA Privacy Office. The Chief, DHA Privacy Office, is the DHA HIPAA Privacy and Security Officer and has the responsibility and authority for the development, implementation, maintenance, oversight, and reporting of privacy and security requirements for PHI. The Chief, DHA Privacy Office shall:

(1) Provide strategic and tactical program direction.

(2) Develop and implement policies and procedures required by Federal legislation that pertain to the privacy and security of PHI, as well as the corresponding DoD policies.

(3) Coordinate across DHA directorates and special staff, with the other individuals assigned security responsibilities to ensure that requirements are appropriately addressed and safeguards are consistent across all DHA Offices.

5. PROCEDURES. See Enclosure 2

6. RELEASABILITY. **Not cleared for public release**. This AI is available to DHA employees and contractor support personnel with Common Access Card authorization on the DHA Intranet.

7. EFFECTIVE DATE. This AI:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it hasn't been reissued or cancelled before this date in accordance with DoD Instruction 5025.01 (Reference (c)).

Douglas J. Robb, DO, MPH
Lieutenant General, USAF, MC, CFS
Director

Enclosures
1. References
2. Procedures

Glossary

# TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
(c) DoD Instruction 5025.01, "DoD Issuances Program," June 6, 2014, as ammended
(d) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003 (or its successor issuance)
(e) DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007 (or its successor issuance)
(f) Parts 160 and 164 (Subparts C, D, and E) of title 45, Code of Federal Regulations (also known as the "HIPAA Rules")
(g) Health Information Technology for Economic and Clinical Health (HITECH) Act
(h) DoD Instruction 5025.01, DoD Directives Program, September 6, 2012 (or its successor issuance)
(i) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007 (or its successor issuance)
(j) DHA Administrative Instruction 71, "Defense Health Agency Incident Response Team and Breach Response Requirements," June 6, 2014

ENCLOSURE 2

PROCEDURES

1. WORKFORCE TRAINING.

a. Pursuant to Reference (d), DHA must train its workforce on their roles and responsibilities for protecting PHI. As such, DHA Privacy Office has developed and implemented a HIPAA awareness and training program for all workforce members and ensures that awareness and training are separate activities.

(1) The DHA HIPAA privacy, security, and breach prevention awareness program exists to heighten the DHA workforce members' familiarity with privacy, security, and breach responsibilities while "training" teaches privacy, security, and breach practices and includes information papers on HIPAA privacy, security, and breach topics, brownbag lectures, list serves, eNews, monthly newsletter to all DHA network users, and periodic email reminders.

(2) The training component of the program consists of formal computer based courses delivered through the Military Health System (MHS) Learn application, or any successor platform chosen for the purpose, administered by the Resource Information Technology Program Office. The application allows the HIPAA Privacy and Security Officer to maintain records documenting the implementation and delivery of the training program including who, where, when, and what was taught.

b. DHA workforce training materials are reviewed and updated, as appropriate, on a periodic basis.

2. POLICY DEVELOPMENT AND REVIEW.

a. DHA must implement and maintain reasonable and appropriate policies and procedures that provide privacy and security protections for all PHI consistent with the HIPAA Rules. These policies and procedures must be up-to-date, signed, disseminated, and include:

(1) A purpose and scope that states expected goals;

(2) Responsibilities; and

(3) Criteria for meeting the requirements.

b. Procedures must also include:

(1) Clarification on where, how, when, about what, and to whom a particular procedure applies;

(2) Clearly defined responsibilities for the affected DHA workforce members; and

(3) Appropriate points of contact.

c. The DHA HIPAA Privacy and Security Officer will ensure that policies are created in compliance with these requirements and will ensure coordination with the DHA and within the DHA workforce.

3. USE AND DISCLOSURE.

a. As required by References (d) and (f), DHA Privacy Office provides individuals with a notice of uses and disclosures of PHI that may be made by the organization and informs them of their rights and the Military Health System's (MHS's) legal duties with respect to PHI.

(1) The notice is provided via the MHS Notice of Privacy Practices (MHS NoPP) and can be found on the DHA Privacy Office website.

(2) Updates are made to the MHS NoPP that reflect any change in HIPAA privacy policy or as required by law.

b. In general, PHI of individuals, both living and deceased, will only be used or disclosed by DHA workforce members for specifically permitted purposes. DHA workforce members are permitted to use and disclose PHI for treatment, payment, or healthcare operations. The DHA health plan workforce and health care providers are permitted to conduct these essential, every day activities without the need for authorization.

c. DHA must account for all disclosures made, except for the following:

(1) To carry out treatment, payment, or health care operations;

(2) To the beneficiary;

(3) Pursuant to a valid authorization;

(4) For facility directories or to persons involved in the beneficiaries care or other notification purposes;

(5) To Federal officials for national security or intelligence purposes;

(6) To correctional institutions or law enforcement officials that have custody of the individual;

(7) That are part of a limited data set; or

(8) Incident to a use or disclosure otherwise permitted or required by the HIPAA Privacy Rule.

d. The DHA PHI Management Tool (PHIMT) is a legacy system that is currently available to DHA workforce members for documenting and retrieving disclosure logs for PHI disclosure accounting purposes. Additional policy, procedures, and templates for accounting of disclosures will be issued as a separate AI.

4. COMPLAINTS.

a. DHA has a process in place for individuals to file complaints concerning DHA or MHS policies and procedures for protecting PHI or compliance with such policies and procedures. DHA's process is managed by the HIPAA Privacy and Security Officer. The process ensures that DHA documents all complaints received and their disposition, if any.

b. Enforcement of the HIPAA Rules is administered through the HHS Office for Civil Rights and could include civil and criminal penalties.

5. SANCTIONS.

a. DHA must ensure that sanction policies are in place and applied appropriately against workforce members who fail to comply with the HIPAA Rules as implemented within DHA, including its HIPAA privacy/security policies and procedures. As part of the policy process, DHA must ensure that the workforce is notified of its sanction policies.

b. The HIPAA Privacy and Security Officer coordinates with the DHA Human Resources (HR) Division and the DHA Office of the General Counsel to ensure that DHA uses standard disciplinary processes, when appropriate, to determine specific sanctions according to the severity and circumstances of violations. The type and severity of sanctions imposed, and the categories of violation, are at the discretion of DHA, but are based on objective criteria as identified in the DHA HR Sanctions Administrative Instruction.

6. BUSINESS ASSOCIATE AGREEMENTS. A DHA business associate is authorized to create, use, receive, maintain, or transmit PHI on behalf of the DHA in accordance with its business associate agreement (BAA), provided appropriate assurances are presented to DHA that the business associate will appropriately use and safeguard the information on DHA's behalf. DHA must ensure satisfactory assurances that meet these requirements are documented through a written contract or other legal arrangement with the business associate (e.g., a BAA or other written arrangement as provided by Reference (d)). Under Reference (g) and the HIPAA Rules, business associates are directly accountable for their compliance with the HIPAA Security Rule and portions of the HIPAA Privacy and Breach Notification Rules. To further this end, the DHA Privacy Office has collaborated with the Contracting Office Directorate to establish uniform

BAA language to be used by contractors with DHA when the subject matter of the contract involves PHI.

7. INCIDENT AND BREACH RESPONSE.

a. DoD 5400.11-R (Reference (i), defines a breach as the "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected," and outlines the steps DoD Components must take in the event of a breach of PII, including PHI. In addition to the requirements outlined in Reference (i), responsibility for breach notification and reporting with respect to PHI expanded in accordance with Reference (g).

b. An "HHS breach," as defined in the HIPAA Rules, differs from the broader definition established in Reference (i). The HIPAA Breach Rule requires notification to be provided to individuals affected by breaches of PHI and requires breaches of unsecured PHI to be reported to HHS.

c. Breaches involving encrypted PHI (whether at rest or in transit) that is compliant with the current DoD standards of encryption, do not invoke the breach reporting requirements under the HIPAA Breach Rule, but still require reporting in accordance with Reference (i). A documented risk analysis is required for all breaches involving PHI to determine whether or not reporting to HHS is required using the DHA Breach Risk Assessment Template published with Reference (j).

d. The HIPAA Breach Rule provisions on breach notification apply equally to all DoD covered entities, including managed care support contractors and other business associates of DoD covered entities. Business associates must continue to follow existing contract requirements by reporting all incidents to the DHA Privacy Office, which will determine if the breach qualifies as reportable to HHS under the provisions of the HIPAA Rules and subsequently report the breach to the Secretary, HHS. In such instances where reporting to HHS is required, the DHA Privacy Office will report the breach to HHS and provide courtesy notification to the appropriate DoD covered entity.

e. The Chief, DHA Privacy Office, also coordinates comprehensive HIPAA breach response and prevention efforts, to include reporting, monitoring, and remediation efforts within the MHS and by DoD covered entities. Additionally, the DHA Privacy Office ensures compliance with related policies and assists in the development of guidance specific to HIPAA breach response, to include DHA AI 71 (Reference (j)) .

f. The Chief, DHA Privacy Office, also conducts an annual incident response team (IRT) exercise involving senior DHA leaders and representatives from other DHA potential IRT representatives to practice individual roles and strengthen joint-organization response readiness.

g. The HIPAA Privacy and Security Officer works with the Cyber Security Division, the Mission Assurance Division, and DHA incident response team leadership in accordance with

Reference (j) to establish appropriate response procedures for all levels of incidents. These procedures demonstrate how DHA will identify and respond to suspected or known privacy and security incidents; mitigate, to the extent practicable, harmful effects of privacy and security incidents; and document incidents and their outcomes.

8. SAFEGUARDS.

a. Appropriate administrative, technical, and physical safeguards are necessary to protect the privacy and security of PHI at DHA. The safeguards must reasonably protect PHI from any intentional or unintentional use, or disclosure that is in violation of the standards, implementation specifications or other requirements of the HIPAA Rules and to limit incidental uses or disclosures.

b. The HIPAA Privacy and Security Officer oversees the requirements for the administrative, technical, and physical safeguards required by the HIPAA Rules within DHA but the execution of the requirements are carried out by multiple departments within DHA.

9. HIPAA PRIVACY AND SECURITY RISK MANAGEMENT.

a. The DHA Health Information Technology Directorate (HIT) performs routine risk assessments throughout the life cycle of information systems and following significant changes to the organizational privacy or security posture. DHA establishes the information management process and related activities as the foundation of the organization's privacy and security programs. The approach to privacy and security requires an assessment of the privacy/security posture of the organization and necessitates working to reduce risks on a continual basis as the environment, and needs of the organization change.

b. The HIPAA Privacy and Security Officer works in conjunction with DHA HIT and the Mission Assurance Division to implement privacy and security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the requirements of the HIPAA Rules.

10. INDIVIDUAL RIGHTS.

a. The References (d) and (f) provides the following rights to individuals:

(1) Right to inspect and copy PHI in a designated record set;

(2) Right to request amendment to PHI in a designated record set;

(3) Right to receive a notice of privacy practices that includes how health information may be used and shared;

(4) Right to request restrictions of PHI that is used or disclosed for certain purposes;

(5) Right to receive confidential communications by alternative means or at alternative locations;

(6) Right to request an accounting of certain disclosures of PHI; and

(7) Right to file a HIPAA complaint directly with the local HIPAA Privacy Officer, or with DHA, and/or with HHS Office for Civil Rights.

b. These rights are limited by the scope of the regulations, as have been and will continue to be explained in HIPAA training and in related DoD and/or DHA issuances. DHA, as a covered entity, is required to have procedures in place to adhere to these individual rights.

# GLOSSARY

## PART I. ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| AI | Administrative Instruction |
| ASD(HA) | Assistance Secretary of Defense for Health Affairs |
| DHA | Defense Health Agency |
| HHS | Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act |
| HIT | Health Information Technology |
| HITECH | Health Information Technology for Economic and Clinical Health |
| HR | Human Resources |
| MHS | Military Health System |

## PART II: GLOSSARY

breach. Actual or possible loss of control, unauthorized disclosure of or unauthorized access to PII, including but not limited to PHI, where persons other than authorized users gain access or potential access to such information for any purpose other than authorized purposes, where one or more individuals will be adversely affected. The foregoing definition is based on the definition of a breach of PII in DoD Privacy Act issuances and does not include an HHS breach, which is defined in this glossary.

business associate. Except as provided below, 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 instruction, 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 instruction; or

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.

A DoD covered entity may be a business associate of another DoD covered entity. This circumstance occurs only when the DoD covered entity is not acting as either a health plan or a provider in its dealings with the other DoD covered entity. An example of this is CHAMPUS/TRICARE's relationships with some of its managed care support contractors. It does not occur when the DoD covered entity is acting as a health plan or a provider. For example, the CHAMPUS/TRICARE network providers are not its business associates.

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 includes 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, "The Department of Defense Detainee Program," September 5, 2006.

covered entity. A health plan or a health care provider who transmits any health information in electronic form in connection with a standard transaction (see Glossary) covered by this instruction, e.g. ACS X12N 837 health care claims, ASC X12N 270/271 eligibility inquiries and responses, and the electronic forms of other standard transactions identified in the Glossary definition of standard transaction. To the extent this instruction prescribes duties to be performed by covered entities, such duties apply only to DoD covered entities.

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.

designated record set. 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.

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.

disclosure. The release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

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. To the extent this instruction prescribes duties to be performed by covered entities, the term refers only to DoD covered entities. All covered entities within the MHS (including both health plans and health care providers) are DoD covered entities and designated as a single covered entity. Not all health care providers affiliated with the Armed Forces are DoD covered entities; among those who are not providers associated with Military Entrance Processing Stations (MEPS) and Reserve components practicing outside the authority of MTFs who do not engage in electronic transactions covered by this instruction (see the definition of standard transactions).

DoD Privacy Act issuances. Current DoD issuances implementing the Privacy Act of 1974 in DoD, as identified by DHA Privacy Office guidance.

employment records. Records that include health information and are maintained by a component of the DoD or other entity subject to this instruction; 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 instruction.

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; and

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 evaluation and development of clinical guidelines outcome, if obtaining general knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities as defined in 42 CFR 3.20; 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 instruction.

Customer service, if PHI is not disclosed except as otherwise permitted by this instruction.

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 shall become a covered entity and due diligence related to such activity.

Consistent with the applicable requirements of References (d) and (f), 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; 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.

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 instruction:

The program that provides health care under the authority of the Department of the Army to members of the Uniformed Services.

The program that provides health care under the authority of the Department of the Navy to members of the Uniformed Services.

The program that provides health care under the authority of the Department of the Air Force to members of the Uniformed Services.

The Supplemental Care Program under 10 U.S.C. 1074c and 32 CFR 199.16 for members of the Army, the Navy, the Marine Corps, and the Air Force who receive health care services from providers other than providers of the Department of Defense.

The TRICARE Prime, TRICARE Extra, and TRICARE Standard health care options offered under 32 CFR 199.17

The health care program for the Uniformed Services under title 10, U.S.C.

The following are also included as health plans:

The TRICARE Dental Program under section 1076a of title 10, U.S.C.

The TRICARE Retiree Dental Program under section 1076c of title 10, U.S.C.

The Continued Health Care Benefit Program under section 1078a of title 10, U.S.C.

The Designated Provider Program under section 1073 note of title 10, U.S.C.

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.

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 Armed Forces 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, liability, accident, automobile, or disability income insurance, or similar insurance coverage.

Any other program whose principal purpose is other than providing, or paying the cost of, health care.

Any other program (other than one listed above 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. The acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. HHS' definition of a breach excludes:

Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a 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 protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

A disclosure of protected health information where a 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.

individual. The person who is the subject of PHI.

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; 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.

law enforcement official. An officer or employee of any agency or authority of the United States, 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; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

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.

NoPP. The notice of the MHS' 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.

organized health care arrangement. An organized health care arrangement is an organized system of health care in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in certain joint activities. The MHS and the U.S. Coast Guard is a single organized health care arrangement.

payment. Except as prohibited by Reference (d), 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; and

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 and/or health plan.

PHI. Individually identifiable health information that, except as provided herein 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 Reference (d) is not PHI.

public health authority. 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 responsible for public health matters as part of its official mandate. The term "public health authority" includes any DoD Component authorized under applicable DoD Regulation to carry out public health activities, including medical surveillance activities.

standard transactions. The transactions covered by this instruction mean the transmission of information between two parties to carry out financial or administrative activities related to health care. They include:

Health care claims or equivalent encounter information.

Health care payment and remittance advice.

Coordination of benefits.

Health care claim status.

Enrollment or disenrollment in a health plan.

Eligibility for a health plan.

Health plan premium payments.

Referral certification and authorization.

First report of injury.

Health claims attachments.

Health care electronic funds transfers (EFT) and remittance advice

Other transactions that the Secretary of HHS may prescribe by regulation.

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.

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.

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 Reference (g).

workforce. Employees, contractor employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a DoD covered entity, business associate, or subcontractor is under the direct control of such entity, whether or not they are paid by the DoD covered entity, business associate, or subcontractor, as the case may be.