



DEFENSE
HEALTH AGENCY

**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS**

7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

SEP - 2 2014

MEMORANDUM FOR LINDA THOMAS, CHIEF, DEFENSE HEALTH AGENCY
PRIVACY AND CIVIL LIBERTIES OFFICE

SUBJECT: Designation of a Defense Health Agency Health Insurance Portability and
Accountability Act Privacy Officer and Health Insurance Portability and
Accountability Act Security Officer

You are hereby designated as the Defense Health Agency's (DHA) Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer and HIPAA Security Officer. The HIPAA of 1996, Public Law 104-191, as well as Department of Defense (DoD) 6025.18-R, "Health Information Privacy Regulation," and any successor issuances, and DoD 8580.02-R, "Health Information Security Regulation," and any successor issuances, require that a covered entity designate a HIPAA Privacy Officer and a HIPAA Security Officer to be responsible for the development and implementation of policies and procedures required under each set of regulations.

As the DHA HIPAA Privacy Officer and HIPAA Security Officer, you have the overall responsibility for: maintaining the privacy, confidentiality, and security of health information, ensuring compliance with State and Federal laws, developing appropriate organizational initiatives; and exercising ethical decision making. You also have signature authority for approval of routine HIPAA privacy and HIPAA security correspondence.

[Signed]

A handwritten signature in black ink, appearing to be "D. Robb", written over a vertical line.

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

**TMA HIPAA Privacy and Security Core Tenets
Policy Statement
(Adopted August 30, 2012)**

BACKGROUND

Pursuant to its authority under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) HIPAA Privacy Rule became effective in 2003 and its HIPAA Security Rule became effective in 2005. Because it is the headquarters for the DoD health benefits program and because of its relationship to the Military Health System (MHS), the TRICARE Management Activity (TMA) is a covered entity under HIPAA and subject to the HIPAA Privacy and Security Rules.

To implement the HIPAA Rules with respect to its healthcare provider and health plan components and functional offices such as TMA, DoD issued the DoD Health Information Privacy Regulation, DoD 6025.18-R (2003), and the DoD Health Information Security Regulation, DoD 8580.02-R (2007). The HIPAA Rules, together with these two DoD regulations, set forth standards and requirements for safeguarding the confidentiality, integrity, and availability of protected health information (PHI) within all DoD covered entity components, as well as the permitted and required uses and disclosures of PHI by such components.

In February 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act became law. The HITECH Act expanded the scope of HIPAA and the HIPAA Privacy and Security Rules. HHS is currently implementing, through regulations amending the HIPAA Privacy and Security Rules, the HITECH Act. To date, it has issued interim final rules on enforcement and on breach notification. Further regulations implementing the HITECH Act are in various stages of development within HHS.

TMA must meet the objectives of all of the HIPAA Privacy and Security Rules to ensure that when PHI is collected, maintained, used, disclosed or transmitted that reasonable and appropriate administrative, physical and technical safeguards have been implemented to ensure integrity, availability and confidentiality. Such measures are in the form of policies and procedures (administrative) as well as technical and physical safeguards and are intended to provide protection against any reasonably anticipated threats or hazards. These safeguards also ensure that the information is used and disclosed only as permitted by the Privacy Rule, and ensure that the TMA workforce complies with the HIPAA training requirements.

This policy and the subsequent Administrative Instructions apply to TMA Directorates, TRICARE Regional Offices (TRO), TRICARE Area Offices (TAO), and all other organizational entities in TMA (collectively referred to as the TMA Offices). It applies to all TMA workforce members including uniformed members, civilian employees, and TRICARE contractors when required by contract.

POLICY OVERVIEW

TMA 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. Confidentiality includes protection against any reasonably anticipated uses or disclosures of such information that are not permitted or required, as well as ensuring that permitted uses and disclosures are in accordance with the HIPAA Privacy Rule.

The requirements of the HIPAA Privacy and Security Rules as implemented within the DoD are extensive; however, the core tenets can be expressed through the following high level activities:

1. HIPAA Privacy/Security Officer

The Director of the TMA Privacy and Civil Liberties Office is the TMA 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 HIPAA Privacy and Security Officer provides strategic and tactical program direction. The HIPAA Privacy and Security Officer is responsible for the development and implementation of the policies and procedures required by Federal legislation that pertain to the privacy and security of PHI, as well as the corresponding DoD Regulations. While more than one individual has security responsibilities at TMA, the HIPAA Security Rule requires that a single individual be designated as having the overall responsibility for PHI. The HIPAA Privacy and Security Officer will coordinate with the other individuals assigned security responsibilities to ensure that requirements are appropriately addressed and safeguards are consistent across all TMA Offices.

2. Workforce Training

TMA must train its workforce on their roles and responsibilities for protecting PHI. As such, TMA has developed and implemented a HIPAA awareness and training program for all members of the workforce. TMA ensures that awareness and training are separate activities. Privacy and security “awareness” exists to continuously heighten the workforce members’ familiarity with privacy and security while “training” teaches privacy and security practices.

The awareness portion of the program includes information papers on HIPAA privacy and security topics, brownbag lectures, list serves, eNews and weekly email reminders. The training component of the program consists of formal computer based courses delivered through the MHS Learn application 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. Workforce training materials are reviewed and updated, as appropriate, on an annual basis.

3. Policy Development and Review

TMA must implement and maintain reasonable and appropriate policies and procedures that provide privacy and security protections for all PHI. 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.

Procedures must also include:

1. Clarification on where, how, when, about what and to whom, a particular procedure applies;
2. Clearly defined responsibilities and expected behaviors for the effected members of the workforce; and
3. Appropriate points of contact.

The HIPAA Privacy and Security Officer will ensure that policies are created in compliance with these requirements and will ensure coordination with all affected TMA Offices.

4. Use and Disclosure

As required by the HIPAA Privacy Rule and DoD 6025.18-R, TMA 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 TMA's legal duties with respect to PHI. This notice is provided by the MHS Notice of Privacy Practices and can be found on the TMA Privacy Office website at: <http://www.tricare.mil/tma/privacy/hipaa-nopp.aspx>. Updates are made to the Notice of Privacy Practice that reflect any change in privacy policy or as required by law.

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

TMA must account for all disclosures made, except for disclosures:

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 HIPAA.

The TMA PHI Management Tool (PHIMT) is a legacy system that is currently available to TMA workforce members for documenting and retrieving disclosure logs for PHI accounting purposes. Additional information regarding the PHIMT can be found at: <http://www.tricare.mil/tma/privacy/ProtectedHealthInformationManagementTool.aspx>. Additional policy, procedures, and templates for accounting of disclosures will be issued as Administrative Instruction #50.

5. Complaints

TMA has a process in place for individuals to make complaints concerning TMA's policies and procedures for protecting PHI or its compliance with such policies and procedures. TMA's process is managed by the HIPAA Privacy and Security Officer. The process ensures that TMA documents all complaints received and their disposition, if any. For more information regarding TMA's HIPAA Privacy complaint process, see: <http://www.tricare.mil/tma/privacy/hipaa-PrivacyComplaint.aspx>

Enforcement of the HIPAA Privacy and Security Rule is administered through the HHS Office for Civil Rights and could include civil and criminal penalties.

6. Sanctions

TMA must ensure that sanction policies are in place and applied appropriately against workforce members who fail to comply with the HIPAA privacy/security policies and procedures of the organization. As part of the policy process, TMA must ensure that the workforce is notified of the sanction policy.

The HIPAA Privacy and Security Officer coordinates with the Human Resource Department and the Office of General Counsel to ensure that TMA 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 TMA.

7. Business Associate Agreements

Business associates of TMA are authorized to create, use, receive, maintain, or transmit PHI on behalf of the organization provided that appropriate assurances are presented to the organization that the business associate will appropriately use and safeguard the information on its behalf. TMA must ensure satisfactory assurances that meet these requirements are documented through a written contract or other legal arrangement with the business associate. Under HITECH, business associates are directly accountable for their compliance with the HIPAA Security Rule and portions of the HIPAA Privacy Rule.

8. Incident Response

The Department of Defense (DoD) 5400.11-R, "DoD Privacy Program," May 14, 2007, 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. In addition to the requirements outlined in the DoD 5400.11-R, responsibility for breach notification and reporting has expanded with the HITECH Act. A "breach," as defined by HHS, differs from the broader definition established by DoD policy. HHS issued guidance in August 2009 for these new requirements in an Interim Final Rule on Breach Notification for Unsecured Protected Health Information ("HHS Breach Rule"). This interim rule includes requirements to provide notification to individuals affected by breaches and to report breaches of unsecured PHI to HHS. Breaches involving encrypted PHI (whether at rest or in transit), that is compliant with the current standards of encryption, do not invoke the breach reporting requirements under the HHS Breach Rule, but will still require reporting in accordance with DoD 5400.11-R. Such instances are typically deemed as low risk breaches using the DoD's standard matrix, the Risk Assessment Model. It should be noted that amendments to various requirements may be implemented when the final rule is published.

These provisions apply equally to MHS Components, including Managed Care Support Contractors and other business associates of MHS-covered entities. Business associates shall continue to follow existing contract requirements by reporting to the TMA Privacy and Civil Liberties Office (TMA Privacy Office), which will determine if the incident qualifies as a breach under the provisions of the HHS Breach Rule and will subsequently report the incident directly to the Secretary, HHS, as appropriate. In such instances where reporting to HHS is required, the TMA Privacy Office, Director, will report the incident to HHS and provide courtesy notification to Component.

The TMA Privacy Office, Director, also coordinates comprehensive breach response efforts, to include reporting, monitoring, and remediation efforts within the MHS. Additionally, the Privacy Office ensures compliance with overarching policies and assists in the development of guidance specific to breach response, to include the TMA Incident Response Team and Breach Notification Policy Memorandum and Administrative Instruction, November 5, 2009.

The TMA Privacy Office, Director, also conducts annual incident response exercises involving senior MHS leaders and representatives from other DoD components to practice individual roles and strengthen joint-organization response readiness. More information on breach reporting requirements can be found on the Breach Response page of the TMA Privacy web site at: <http://www.tricare.mil/tma/privacy/breach.aspx>.

The HIPAA Privacy and Security Officer works with the Information Assurance Office, the Physical Security Office, and TMA leadership to establish appropriate response procedures for all levels of incidents. These procedures demonstrate how TMA 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.

9. Safeguards

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

The HIPAA Privacy and Security Officer oversees the requirements for the administrative, technical, and physical safeguards required by HIPAA but the execution of the requirements are carried out by multiple departments within TMA. The technical safeguards are primarily managed by the Network Operations division under the Chief Information Officer and the physical safeguards are under the cognizance of the TMA Security Officer under the Office of Administration, Security and Safety Division. The administrative safeguards are addressed through several policies, procedures and processes within TMA.

10. HIPAA Privacy and Security Risk Management

TMA performs routine risk assessments throughout the life cycle of information systems and following significant changes to the organizational privacy or security posture. TMA 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.

The HIPAA Privacy and Security Officer works in conjunction with the Technology Management, Integration and Standards Office to implement privacy and security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Privacy and Security Rules requirements.

11. Individual Rights:

The HIPAA Privacy Rule and DoD 6025.18-R 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
7. Right to file a complaint with TMA and/or with the Office for Civil Rights

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 issuances. TMA, as a covered entity, is required to have procedures in place to adhere to these individual rights.