THE ASSISTANT SECRETARY OF DEFENSE

1200 DEFENSE PENTAGON
WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

JUN 27 2006

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY (M&RA)
ASSISTANT SECRETARY OF THE NAVY (M&RA)
ASSISTANT SECRETARY OF THE AIR FORCE (M&RA)

SUBJECT: Health Insurance Portability and Accountability Act Security Compliance

This policy memorandum implements the Department of Health and Human Services Security Standards, Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191) Final Rule (45 Code of Federal Regulations, Parts 160, 162 and 164). In order to establish this policy within the Department of Defense (DoD), a Health Information Security Regulation will follow within the next 180 days.

The HIPAA Security Rule mandates the standards for the integrity, confidentiality and availability of all electronic Protected Health Information (ePHI), and requires that reasonable and appropriate administrative, physical, and technical safeguards be implemented to protect this health information. Under provisions of the HIPAA Security Rule, organizations must ensure the confidentiality, integrity, and availability of ePHI that the organization creates, receives, maintains, or transmits. The HIPAA Security Rule also charges organizations to protect ePHI against any reasonably anticipated threats or hazards to the security or integrity of such information.

DoD organizations must protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the DoD Health Information Privacy Regulation (DoD 6025.18-R), and ensure compliance with the HIPAA Security Rule by its workforce through application of the Policy Guidance contained herein. Protection will be accomplished through the implementation and maintenance of reasonable and appropriate policies and procedures that comply with the requirements of the HIPAA Security Rule with respect to all ePHI. The rule requires compliance by April 20, 2005.

Organizations must maintain the policies and procedures implemented to comply with the HIPAA Security Policy Guidance in written form and a written record (both of which can be electronic) of the actions, activities, or assessments that require documentation by the HIPAA Security Rule. Documentation must be retained for six years from the date of their creation or the date when they were last in effect, whichever is later.

HA POLICY: 06-010

Documentation must also be made available to those persons responsible for implementing the procedures to which the documentation pertains. This documentation will be reviewed by organizations, at a minimum, annually, and updated upon issuance of the DoD Regulation implementing the HIPAA Security Rule, and as needed in response to environmental or operational changes affecting the security of the ePHI.

The policy guidance outlining how to implement reasonable and appropriate administrative, physical, and technical safeguards can be found in this memorandum's Attachment. The requirements herein have been communicated in detail to the Uniformed Services through the HIPAA Security Integrated Process Team during the past 18 months. I note that many requirements required by this Policy Guidance are required by various DoD and Service policies as well. HIPAA requires documentation of compliance related to these specific standards and safeguards. HIPAA Security allows the use of alternative measures where compliance can be demonstrated from the documentation from another source that fulfills the HIPAA Security requirements.

My point of contact for this initiative is TMA Privacy Officer, Mr. Samuel P. Jenkins at *Sam.Jenkins@tma.osd.mil*.

William Winkenwerder, Jr., MD

Attachments
As stated

cc:
Surgeon General of the Army
Surgeon General of the Navy
Surgeon General of the Air Force
Director, Health and Safety, US Coast Guard
Reserve Component Surgeon General of the Army
Chief, Naval Reserve
Command Surgeon, Air Force Reserve
Surgeon General of the Public Health Service
Deputy Director, TRICARE Management Activity

Policy Guidance for Implementation of the HIPAA Security Rule

The following paragraphs outline the responsibilities of DoD and the Service Surgeons General regarding compliance with the HIPAA Security final Rule. These responsibilities were developed through analysis of the HIPAA Security final Rule and MHS business processes by the HIPAA Security Integrated Project Team, which included representatives from the Services and TMA.

1. Administrative Safeguards

A. Implement a security management process, including policies and procedures, to prevent, detect, contain, and correct security violations.

(1) Conduct a risk analysis that includes an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of all ePHI created, received, stored, or transmitted by the organization.

(2) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Organizations must ensure the confidentiality, integrity and compliance by its workforce and protect against reasonably anticipated threats and hazards to the security of ePHI and unauthorized uses and disclosures of ePHI.

(3) Ensure that sanction policies are in place and applied appropriately against workforce members who fail to comply with the security policies and procedures of the organization.

(4) Implement procedures for regular review of records of information system activity such as audit logs, access reports, and security incident tracking reports.

B. Identify and assign, in writing, a HIPAA Security Officer, who is the security official for the organization responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule. More than one individual may be given security responsibilities, but a single individual must be designated as having the overall and final responsibility.

C. Implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI. Prevent those workforce members who do not have authorized access, either physical or electronic, from obtaining contact with ePHI.

(1) Implement procedures for the authorization and/or supervision of workforce members. A workforce member working with or in locations accessible to ePHI must either be authorized to be there, supervised while there, or both.

(2) Implement procedures to determine the appropriate access of workforce members to ePHI.

(3) Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by the organization's workforce clearance procedure.

D. Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of Sections 3541–3544 of Title 44, United States Code and the DoD Health Information Privacy Regulation (DoD 6025.18-R).

(1) Implement policies and procedures for granting an individual access to ePHI through multiple venues that include access to a workstation, transaction, program, process, or other mechanism. Include clear delineation on the required authorizations and clearances needed before an account can be established.

(2) Based upon the organization's access authorization policies, implement additional policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

E. Develop and implement a security awareness and training program for all members of the workforce that complements the requirements of DoD Information Assurance Training, Certification, and Workforce Management Directive (DoD 8570.1).

(1) Implement annual (or more frequently, if necessary) security updates that serve as a security reminder to increase security awareness. Security reminders include e-mail messages, newsletters, posters, etc.

(2) Implement security awareness and training that cover procedures for guarding against, detecting, and reporting malicious software.

(3) Implement security awareness and training that cover procedures for monitoring log-in attempts and reporting discrepancies to the appropriate security official.

(4) Implement security awareness and training that cover procedures for creating, changing, and safeguarding passwords. Train personnel in the organization's

password policies; and how to create, change, and protect passwords including the handling of lost or compromised passwords.

F. Implement policies and procedures to address security incidents.

(1) A security incident is defined, for the purposes of this memorandum, as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system." Security incidents include, but are not limited to, policy violations by users, denial of service attacks, intrusions, and unauthorized disclosures.

(2) Establish response procedures for all levels of incidents that demonstrate how the organization will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents; and document security incidents and their outcomes.

G. Establish and review, annually, policies and procedures for responding to an emergency or other occurrence such as fire, vandalism, system failure, or natural disaster that damages systems that contain ePHI. Review and update the Contingency Plan and all of the subsections of this requirement as needed.

(1) Establish policies and procedures to create and maintain retrievable exact copies of ePHI to ensure that information will not be lost in the event of a major system loss.

(2) Establish and implement, annually, policies and procedures to restore any loss of data. Contingency plans must include a strategy and method for recovering lost or inaccessible PHI in a timely manner after a disaster.

(3) Establish and implement, annually, policies and procedures to enable continuation of critical business processes for the protection of the security of ePHI while operating in emergency mode. Contingency plans must contain an Emergency Operations Plan that establishes an alternate means of ePHI during an emergency.

(4) Implement procedures for annual testing and revision of written contingency plans to look for any weaknesses. Revise the plan based on the results of testing, if necessary, and to ensure that it remains appropriate as business processes and the environment change over time.

(5) As part of an organization's risk assessment, assess the relative criticality of specific applications and data in support of other contingency plan components.

Utilize the results of this analysis to assign priority to information resources and determine the best strategy to protect those resources.

H. Perform an annual (at a minimum) technical and non-technical evaluation of the security program based upon the HIPAA Security Rule and in response to environmental or operational changes affecting the security of ePHI. Establish the extent to which the organization's security policies and procedures meet the requirements of the HIPAA Security Rule.

I. Business associates are authorized to create, receive, maintain, or transmit ePHI on behalf of the organization provided that assurances are presented to the organization that the business associate will appropriately safeguard the information on its behalf. Satisfactory assurances that meet the applicable requirements of the HIPAA Security Rule must be documented through a written contract or other legal arrangement with the business associate.

(1) The contract or other arrangement must require the business associate to:

(a) Implement administrative, physical and technical safeguards that will protect the ePHI that the business associate creates, receives, maintains, or transmits on behalf of the organization;

(b) Ensure that all agents or subcontractors to whom the business associate provides ePHI to will also implement safeguards to protect the information,

(c) Report all security incidents to the organization as directed in the organization's contract and,

(d) Authorize termination of the contract if the organization finds that the business associate has violated the terms of the contract. The organization may omit this authorization of the termination if such authorization is inconsistent with the statutory obligations of the organization or its business associate.

(2) An organization that becomes aware of a violation of its contract or other arrangement is required to:

(a) Take the necessary steps to mitigate the violation

(b) Terminate the contract or arrangement if those steps do not successfully end the violation

(c) Report the problem to the appropriate chain of command if termination is not reasonable.

(3) When an organization and its business associate are both governmental entities, the organization is in compliance with the HIPAA Security Rule if the organization enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms that accomplish the objectives of this regulation or other laws (including regulations adopted by the organization or its business associate) containing requirements applicable to the business associate that accomplish the objectives of this regulation.

(4) If a business associate is required by law to perform a function or activity on behalf of an organization, or to provide a service to an organization, the organization may permit the business associate to create, receive, maintain, or transmit ePHI on its behalf to the extent necessary to comply with the legal mandate. The organization must attempt in good faith to obtain satisfactory assurances that the business associate will appropriately safeguard the information on its behalf and document the attempt. The organization must also document any reason why these assurances cannot be obtained.

2. Physical Safeguards

A. Implement policies and procedures to limit physical access to information systems or biomedical devices and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(1) Establish and implement, annually, procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(2) Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(3) Implement procedures to control and validate identification and authentication of a person's access to facilities based on their role or function, including visitor control and control of access to firmware, hardware or software programs for testing and revision.

(4) Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, or locks).

B. Implement policies and procedures concerning workstations that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or a class of workstation that can access ePHI.

C. Implement physical safeguards for all workstations that access ePHI. Ensure that workstation access is only granted to authorized users and prevent workstation access to unauthorized users.

D. Implement policies and procedures for device and media controls that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility.

(1) Implement policies and procedures to address the final disposition of ePHI or the hardware or electronic media on which it is stored. Procedures must include approved methods of disposal such as use of commercial or public disposal services, sale or donation of electronic devices and the process for ensuring that ePHI processed by or stored on the hardware and electronic media is no longer accessible.

(2) Implement procedures for removal of ePHI from electronic media before the media is made available for re-use. Methods for removing ePHI include reformatting, writing over existing data, and use of special demagnetizing (degaussing) equipment.

(3) Maintain a record of the movements of hardware and electronic media and any person responsible therefore. Implement procedures for safely managing electronic devices and media, including records of who has the devices or media, when they had possession, and where they kept the devices or media from the time of original receipt to time of final disposal or transfer to another entity.

(4) Create a retrievable, exact copy of ePHI before movement of equipment.

3. Technical Safeguards

A. Implement technical policies and procedures for information systems and electronic devices containing PHI that allows access only to those persons or software programs that have been granted access rights as specified in the organization's information access policies.

(1) Assign a unique name and/or number for identifying and tracking user identity.

(2) Establish and implement, as needed, procedures for obtaining necessary ePHI when standard procedures fail due to a crisis situation including system failure or the unavailability of authorized users.

(3) Assess the need to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Based on the organization's risk assessment, implement an automatic logoff if reasonable and appropriate. If implementing an automatic logoff is not reasonable and appropriate, document why it is not reasonable and appropriate and implement an equivalent alternative measure. Document that alternative measure and how it achieves the same objective.

(4) Assess the need to implement a mechanism to encrypt and decrypt ePHI at rest and during transmission as a means of controlling access to the ePHI. Based on the organization's risk assessment, implement a mechanism to encrypt and decrypt ePHI at rest if reasonable and appropriate. If not reasonable and appropriate, document why and implement an equivalent alternative measure. Document the alternative measure and how it achieves the same objective.

B. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

C. Deploy and use technical policies and procedures to protect ePHI from improper or unauthorized access, use, disclosure, modification, alteration or destruction.

(1) Technical policies and procedures include access controls, virus protection, and encryption.

(2) Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. Employ technical mechanisms such as check sums, message authentication codes, and digital signatures to authenticate the integrity of ePHI in automated information systems.

D. Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. Install and use technical procedures that verify the identification and authentication of human users and other machines that transfer or request information.

E. Implement technical security mechanisms to guard against unauthorized access, use, disclosure, modification, alteration, or destruction to PHI that is being transmitted over an electronic communications network. Assess and install appropriate technical controls that mitigate threats to data security in transit over all types of networks including, but not limited to, wireless networks, the Internet, corporate intranets, dedicated lease lines, and dial-up connections.

(1) Implement security mechanisms to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of. Integrity controls must provide assurance that a transmitted message arrives at its destination exactly as it left its origin.

(2) Assess the need to encrypt ePHI in transit to protect the confidentiality and integrity of the data during transmission over a network or other electronic means. Based on the organization's risk assessment, implement encryption of ePHI if reasonable and appropriate. If not reasonable and appropriate, document why and implement an equivalent alternative measure. Document the alternative measure and how it achieves the same objective.