TMA Privacy Office
Information Paper

SECURITY MANAGEMENT PROCESS

HIPAA Security ♦ February 2012

I. *Supporting Regulations for Security Management Process*

A. The U.S. Department of Health and Human Services (HHS) Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule establishes the requirements for covered entities to develop policies and procedures to implement a security management process as a part of their administrative safeguards. See 45 CFR 164.308(a)(1).

B. The Department of Defense (DoD) Health Information Security Regulation (DoD 8580.02-R) implements the aforementioned section of the HHS HIPAA Security Rule within the Military Health System (MHS). See C2.2.

II. *Definitions Associated with Security Management Process*

A. Availability: The property that data or information is accessible and useable upon demand by an authorized person.

B. Confidentiality: Information (as property) is not made available or disclosed to unauthorized individuals, entities or processes.

C. Covered Entity: A health plan or a healthcare provider within the MHS that transmits any health information in electronic form in connection with one of the transactions specified in the HHS implementing rules, which carry out financial or administrative activities related to healthcare.

D. Integrity: The property that data or information has not been altered or destroyed in an unauthorized manner; implementing policies and procedures to protect electronic protected health information (ePHI) from improper modification or destruction.

E. Military Health System (MHS): All DoD health plans and all DoD healthcare 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 TRICARE Management Activity (TMA), the Army, the Navy, or the Air Force.

F. Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in electronic or any other form or medium, except as otherwise contained in employment records held by a covered entity in its role as an employer.

G. Risk Analysis: Examination of information to identify the risk to an information system.

H. Risk Management: The process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

I. Safeguards: The appropriate administrative, technical, and physical controls that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures.

J. Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

K. Security Policy: The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system.

L. Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

III. Guidance For Security Management Process

A. Background: The DoD Regulation 8580.02-R, "Health Information Security Regulation," outlines the procedures required for the covered entities to implement a security management process as a part of their administrative safeguards.

B. Process: The process includes implementing "policies and procedures to prevent, detect, contain and correct security violations."

C. Approach: The security management process and its related implementation specifications form the foundation of a covered entity's entire security program. This standard mandates a "life cycle approach" to security; that is, an organization must assess its security posture and work to reduce its risks on a continual basis as the security environment and needs of the organization change. (Refer to HIPAA Security Information Paper "Specifications: Standards and Implementation," February 2012)

D. Establishment: Establish the security management process and related activities as the foundation of the organization's security program. Utilize a life cycle approach to security that requires an assessment of the security posture of the organization and work to reduce risks on a continual basis as the security, environment, and needs of the organization change.

E. Risk Analysis: 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. A risk analysis should include:

   1. A threat assessment, vulnerability pairing, and residual risk determination.

   2. Consideration of both organizational and technical assessments that address all areas of security, including losses caused by unauthorized uses and disclosures, as well as losses of data integrity or accuracy.

F. Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule. In doing so, the organization should:

   1. 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.

   2. Develop plans and take actions to implement safeguards in response to the findings of the risk analysis. Conduct reassessments regularly to determine the effectiveness of implemented safeguards.

G. Sanction Policy: 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. Ensure that the workforce is notified of the sanction policy. Use 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 the organization.

H. Information System Activity Review: Implement procedures for regular review of records of information system activity such as audit logs, access reports, and security incident tracking reports. Other requirements include:

   1. Examine records of system use (such as audit and system logs) for potential breaches of security policy.

   2. Determine the frequency of reviews for both automated and manual logs.

   3. Review reports based on the organization's risk analysis and risk process determination.