



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



Security Management

HIPAA Security Information Paper ♦ March 2010

PURPOSE:

The purpose of this paper is to elaborate on the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Rule “Security Management Process” requirements as specified by DoD Regulation 8580.02-R, “Health Information Security Regulation”, (reference (a)). The following policy outlines the procedures which are required.

BACKGROUND:

The HIPAA Security Rule requires covered entities, i.e., MHS, to implement a security management process as a part of their administrative safeguards. The HIPAA Security Rule defines that process as the implementation of “policies and procedures to prevent, detect, contain and correct security violations.” 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 to say, 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.

POLICY:

Covered entities shall implement a security management process, including policies and procedures, to prevent, detect, contain, and correct security violations.

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.

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 electronic protected health information (ePHI) created, received, stored, or transmitted by the organization.

Include a threat assessment, vulnerability pairing, and residual risk determination in the risk analysis. Consider both organizational and technical assessments that address all areas of security in the



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



Security Management

HIPAA Security Information Paper ♦ March 2010

place, including losses caused by unauthorized uses and disclosures, as well as losses of data integrity or accuracy.

Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with reference (a). 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.

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.

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.

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.

Examine records of system use (such as audit and system logs) for potential breaches of security policy. Determine the frequency of reviews for both automated and manual logs. Reports must be reviewed based on the organization’s risk analysis and risk process determination.

REFERENCES:

- (a) DoD 8580.02-R, “Health Information Security Regulation”, July 12, 2007