



# TMA Privacy Office Information Paper

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



## Specifications: Standards and Implementation

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 requirements for “Standards and Implementations Specifications” as specified by DoD Regulation 8580.02-R, “Health Information Security Regulation”, (reference (a)). The following policy outlines the procedures which are required.

### **BACKGROUND:**

#### **General Requirement**

The HIPAA Security Rule divides its protections into three safeguard categories: administrative, physical and technical safeguards. The three safeguard categories are further divided into standards that describe what each covered entity must do to meet the objectives of the Security Rule. In some cases, the standard itself contains enough information to describe implementation requirements, so there is no separate specification. Other standards have associated “implementation specifications” that expand on or explain what is required by the standard. Covered entities must implement safeguards that ensure compliance with the standards and implementation specifications included in each category.

#### **Safeguard Categories**

Administrative safeguards are “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information (ePHI) and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

Physical safeguards are “physical measures, policies and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

Technical safeguards are “the technology and the policy and procedures for its use that protect ePHI and control access to it.”

### **POLICY:**

For a covered entity, all standards are required and must be met. Implementation specifications are either “required” or “addressable.” There are three implementation specifications that are “addressable.” A required implementation specification means just that; it must be done. An addressable implementation



# TMA Privacy Office Information Paper

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



## Specifications: Standards and Implementation

### HIPAA Security Information Paper ♦ March 2010

specification must be “assessed” and “reasonable and appropriate” action taken. Each covered entity must base their decision as to what is “reasonable and appropriate” on its risk analysis, its mitigation strategy for those risks, the security measures already in place, and the costs of alternatives. Once that has been done, the following decision steps apply. If an addressable implementation specification is determined to be:

- Reasonable and appropriate given the circumstances of the covered entity, it must be implemented;
- Unreasonable or inappropriate, but the standard cannot be met without it, then an alternative measure that accomplishes the same end must be put in place;
- Unreasonable or inappropriate, or simply not applicable to the situation, and the standard can be met without the specification or alternative, then nothing beyond the standard needs to be put in place.

In all cases the covered entity must document how it is meeting the standards and implementation specifications. The rationale for the selection of an alternative safeguard, or to not implement anything at all, must be documented with particular thoroughness.

#### **Standards Matrix**

The standards and specifications are presented in the matrix below. All standards are required. The implementation specifications associated with some standards provide additional detail when needed and are either required or addressable.

#### **REFERENCES:**

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

<b>Standard(s)</b>	<b>Code of Federal Regulations (CFR) Section</b>	<b>Implementation Specification (N/A) = Not Applicable to DoD (A) = Addressable</b>
<b>Administrative Safeguards</b>		
Security Management Process	164.308(a)(1)	Risk Analysis Risk Management Sanction Policy Information System Activity Review
Assigned Security Responsibility	164.308(a)(2)	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision Workforce Clearance Procedure Termination Procedures
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (N/A) Access Authorization Access Establishment and Modification
Security Awareness and Training	164.308(a)(5)	Security Reminders Protection from Malicious Software Log-in Monitoring Password Management
Security Incident Procedures	164.308(a)(6)	Response and Reporting
Contingency Plan	164.308(a)(7)	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality Analysis
Evaluation	164.308(a)(8)	None
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement
<b>Physical Safeguards</b>		
Facility Access Controls	164.310(a)(1)	Contingency Operations Facility Security Plan Access Control and Validation Procedures Maintenance Records
Workstation Use	164.310(b)	None
Workstation Security	164.310(c)	None
Device and Media Controls	164.310(d)(1)	Disposal Media Re-Use Accountability Data Backup and Storage
<b>Technical Safeguards</b>		
Access Controls	164.312(a)(1)	Unique User Identification Emergency Access Procedure Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	None
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI
Person or Entity Authentication	164.312(d)	None
Transmission Security	164.312(e)(1)	Integrity Controls Encryption (A)