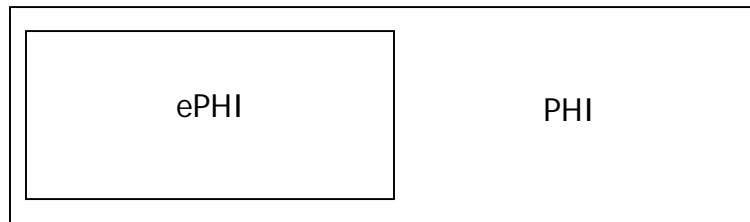


HIPAA SECURITY OVERVIEW

Summer 2005

What do the Security Rules cover?

The Security Rules build upon and add to the HIPAA Privacy policies and procedures already adopted by the covered entity. They specifically focus upon electronic protected health information (“ePHI”). Electronic PHI is a subset of the information protected for HIPAA Privacy purposes. HIPAA Privacy protects “protected health information (PHI)” while the Security Rules protect PHI that is stored or transmitted electronically.



For this purpose, hard drives in software programmable computers (e.g., office computers, hand held personal computers, portable computers), voice response and faxback systems, and email systems are all included within “electronic.” However, memories in copy machines, fax machines, and phone messaging, and most paper fax transmissions are not included within “electronic.”

What are the goals of HIPAA Security?

The HIPAA Security requirements are intended to accomplish the following goals:

- Ensure the confidentiality, integrity, and availability of ePHI the covered entity creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of the ePHI.
- Protect against reasonably anticipated uses or disclosures of ePHI not otherwise permitted or required.

The HIPAA Security requirements provide the covered entity with a great deal of flexibility regarding how to accomplish these goals.

What do the Security Rules require and how are they organized?

The **HIPAA Security Rules** consists of three main categories (administrative safeguards, physical safeguards, technical safeguards) with identified objectives within each. Each identified objective is stated in terms of a mandatory **standard**. Each standard in turn may have one or more **implementation specifications** which may or may not be mandatory; if not mandatory (m), then addressable (a). The standard and the implementation specifications must be reflected in the covered entity's policies and procedures. In some cases, this can be done by amended the existing HIPAA Privacy policies and procedures (see sample attached). In other cases, policies and procedures unique to HIPAA Security must be developed.

Administrative Safeguards

Security Management Process

Standard – prevent, detect, contain and correct security violations

Implementation Specifications:

- Risk Analysis/Assessment (m)
- Risk Management (m)
- Sanction Policy (m)
- Information System Activity Review (m)

Assigned Security Responsibility

Standard – identify security official

Workforce Security

Standard – ensure appropriate access or lack of access to ePHI by workforce

Implementation Specifications:

- Authorization and/or Supervision (a)
- Workforce Clearance Procedure (a)
- Termination Procedures (a)

Information Access Management

Standard – implement procedures for authorizing access to ePHI

Implementation Specifications:

- Isolating Health Care Clearinghouse Function (m)
- Access Authorization (m)
- Access Establishment and Modification (a)

Security Awareness and Training

Standard – security awareness training for workforce

Implementation Specifications:

- Security Reminders (a)
- Protection from Malicious Software (a)
- Log-in Monitoring (a)
- Password Management (a)

Security Incident Procedures

Standard – address security incidents

Implementation Specifications:

- Response and Reporting (m)

Contingency Planning

Standard – respond to an emergency or other occurrence that damages systems that contain ePHI

Implementation Specifications:

- Data Backup Plan (m)
- Disaster Recovery Plan (m)
- Emergency Mode Operations Plan (m)
- Testing and Revision Procedure (a)
- Applications and Data Criticality Analysis (a)

Evaluation

Standard – perform initial and periodic technical and non-technical evaluation (required to establish extent to which security policies and procedures meet requirements)

Business Associate Contracts and Other Arrangements

Standard – obtain satisfactory assurances that business associate will appropriately safeguard ePHI before permitting associate to create, receive, maintain, or transmit ePHI

Implementation Specifications:

Written Contract or Other Arrangement (m)

Physical Safeguards

Facility Access Controls

Standard – allowing and limiting appropriate physical access to electronic information systems and facilities that house them

Implementation Specifications:

Contingency Operations (a)

Facility Security Plan (a)

Access Control and Validation Procedures (a)

Maintenance Records (a)

Workstation Use

Standard – specify functions of, manner in which functions are to be performed by, and physical attributes of workstations with access to ePHI

Workstation Security

Standard – restrict access to workstations with access to ePHI to authorized users

Device and Media Controls

Standard – control the receipt, removal, and movement of hardware and electronic media containing ePHI

Implementation Specifications:

Disposal (m)

Media Re-use (m)

Accountability (a)

Data Backup and Storage (a)

Technical Safeguards

Access Control

Standard – implement technical procedures to restrict access to electronic information systems maintaining ePHI to authorized persons and/or software programs

Implementation Specifications:

Unique User Identification (m)

Emergency Access Procedure (m)

Automatic Log-off (a)

Encryption and Decryption (a)

Audit Control

Standard – implement hardware, software, and/or procedural mechanisms to record and examine activity in electronic systems containing ePHI

Integrity

Standard – protect ePHI from improper alteration or destruction

Implementation Specifications:

Mechanism to Authenticate ePHI (a)

Personal or Entity Authentication

Standard – authenticate identity person or entity seeking access to ePHI

Transmission Security

Standard – implement technical measures to guard against unauthorized access to ePHI during transmission

Implementation Specifications:

Integrity Controls (a)

Encryption (a)

What steps should a health plan take to comply with the Security Rules?

Risk Assessment. The focus of the Security Rules is the protection of the confidentiality, integrity, and availability of ePHI. We recommend, as a first step to HIPAA Security compliance, the covered entity identify ePHI and perform a risk assessment with respect to the pathways through which the ePHI travels.

Policies and Procedures. As with HIPAA Privacy, HIPAA Security requires the development, adoption, and implementation of written policies and procedures. In some cases, compliance involves updating and expanding existing policies and procedures already in place for purposes of HIPAA compliance (e.g., sanctions, training, record retention, complaint process, business associates and their sub-contractors). In other cases, compliance with the Security Rule requires the addition of new policies and procedures specifically directed at electronically stored and transmitted information. More so than HIPAA Privacy, HIPAA Security involves a more individualized assessment and application by the covered entity.

Plan Amendment. As with HIPAA Privacy, HIPAA Security requires the review and amendment of plan documentation. The Security Rule requires amendment of the plan to reflect the protection of ePHI. Other documentation (e.g., notices, enrollment materials, summary plan descriptions) that has been provided to persons receiving coverage under the plan should also be reviewed for consistency and adjusted if necessary.

Business Associate Agreements. As with HIPAA Privacy, HIPAA Security requires the identification of business associates. For purposes of the Security Rules, business associates are third parties contracted to perform functions on behalf of the covered entity that involve ePHI. Not all business associates identified for purposes of HIPAA Privacy will necessarily be business associates for purposes of the Security Rules.

In addition, the written agreement between the covered entity and the business associate must basically obligate the business associate to handle the ePHI in no less a protected manner than the covered entity must handle it. This applies regardless of whether there is a separate, stand alone agreement (e.g., business associate agreement) or the provisions are incorporated into an existing agreement, such as a service agreement.

Training & Awareness. As with HIPAA Privacy, HIPAA Security requires the covered entity's workforce be trained regarding HIPAA Security.

Security Officer. As with HIPAA Privacy, HIPAA Security requires the appointment of a Security Officer, vested with the responsibility for implementation and oversight of the HIPAA Security Rules.