HIPAA Security Final Rule Overview

March 27, 2003

Karen Trudel

Publication Information

- Printed in Federal Register 2/20/03
  - Volume 68, No. 34, pages 8334 - 8381
- Effective Date 4/21/03
- Compliance Date 4/21/05 (4/21/06 for Small Health Plans)
- Document can be located at www.cms.hhs.gov/hipaa/hipaa2

Purpose

- Ensure integrity, confidentiality and availability of electronic protected health information
- Protect against reasonably anticipated threats or hazards, and improper use or disclosure

Scope

- All electronic protected health information (EPHI)
- In motion AND at rest
- All covered entities

Security vs. Privacy

- Closely linked
- Security enables Privacy
- Security scope larger – addresses confidentiality PLUS integrity and availability
- Privacy scope larger – addresses paper and oral PHI

Security Standards General Concepts

- Flexible, Scalable
  - Permits standards to be interpreted and implemented appropriately from the smallest provider to the largest plan
- Comprehensive
  - Cover all aspects of security – behavioral as well as technical
- Technology Neutral
  - Can utilize future technology advances in this fast-changing field

Public Comments

- Widespread support for general concepts
- Need for more flexibility
- Too many requirements

Major Changes from NPRM

- Consolidated and tightened requirements
- Added flexibility
  - Concept of "addressability"
- Coordinated with privacy
  - "Chain of Trust" agreement now handled via business associate agreement

Standards

- Standards are general requirements
- Eighteen administrative, physical and technical standards
- Four organizational standards (conditional)
  - Hybrid entity, affiliated entities, business associate contracts, group health plan requirements
- Two overarching standards
  - Policies and procedures, documentation

Standards vs. Implementation Specifications

- Implementation specifications are more specific measures that pertain to a standard
- 36 implementation specifications for administrative, physical and technical standards
  - 14 mandatory, 22 addressable
- Implementation specifications may be:
  - Required
  - Addressable

Required vs. Addressable

- **Required** – Covered entity MUST implement the specification in order to successfully implement the standard
- Addressable – Covered entity must:
  - Consider the specification, and implement if appropriate
  - If not appropriate, document reason why not, and what WAS done in its place to implement the standard

Standards May Have

- No separate implementation specification – in that case the standard is also the implementation specification (and must be implemented)
- One or more implementation specifications that are all required
- One or more implementation specifications that are all addressable
- A combination of required and addressable implementation specifications

Bottom Line…

- All standards MUST be implemented
- Using a combination of required and addressable implementation specifications and other security measures
- Need to document choices
- This arrangement allows the covered entity to make its own judgments regarding risks and the most effective mechanisms to reduce risks

Example: No Implementation Specification

- Assigned Security Responsibility
  - No additional specifics needed

Example: All Implementation Specifications Required

- Security Management Process
  - Requires risk analysis, risk management, sanction policy, and information system activity review

Example: All Implementation Specifications Addressable

- Security Awareness and Training
  - Specific topics are addressable: security reminders, protection from malicious software, log-in monitoring and password management
  - Even if none of those topics are relevant, the covered entity must still conduct training
  - Covered entity has choices regarding – how training is provided (computer-based, formal classroom, at staff meetings, etc.) and relevant content

Example: Combination of Required and Addressable

- Device and Media Controls
  - Disposal and media reuse specifications are required
  - Accountability and data backup and storage are addressable

Other Changes

- Encryption over open network is now addressable
- Requirement for Certification changed to Evaluation
- Electronic signature standard not adopted at this time

Outreach

- Will develop technical assistance materials
- Working on security video
- Special target audience is small providers

- Questions?