HIPAA Security:
Complying with the HIPAA Security Rule Implementation Specifications – Are You Correctly Addressing Them?

The Seventh National

HIPAA Summit

Monday, September 15, 2003

Tom Walsh, CISSP

Tom Walsh Consulting, LLC

6108 West 121 Street ◆ Overland Park, KS 66209

Phone: 913-696-1573 ◆ e-mail: twalshconsulting@aol.com

HIPAA SECURITY RULE

Comprehensive, Flexible, Scalable, Technology Neutral

- Administrative Safeguards (55%)
  - 12 Required, 11 Addressable
- Physical Safeguards (24%)
  - 4 Required, 6 Addressable
- Technical Safeguards (21%)
  - 4 Requirements, 5 Addressable

Security Rule Sections
§164.304 – Definitions
§164.306 – Security Standards: General Rules
§164.308 – Administrative safeguards
§164.310 – Physical safeguards
§164.312 – Technical safeguards
§164.314 – Organizational requirements
§164.316 – Policies and procedures and documentation requirements
§164.318 – Compliance dates

Addressable Implementation Specifications

"In meeting standards that contain addressable implementation specifications, a covered entity will ultimately do one of the following:

- Implement one or more of the addressable implementation specifications;
- Implement one or more alternative security measures;
- Implement a combination of both; or
- Not implement either an addressable implementation specification or an alternative security measure."

Key Concepts – Security Rule

- Risk Analysis – Determines the appropriate means of compliance
  - Does not imply that organizations are given complete discretion to make their own rules
- Covered entities must assess if an implementation specification is reasonable and appropriate

Privacy versus Security

- **Parallels the Privacy Rule except:**
  - **Security Rule covers only electronic protected health information (ePHI)**
  - **Privacy Rule applies to PHI in paper, oral, and electronic form**
- **Security standards extend to the members a covered entity's workforce even if they work at home**
- **Requires a minimum level of documentatic that must be retained for six years**

ADMINISTRATIVE SAFEGUARDS

Security Management Process

- **Risk Analysis (R)**

  Assesses its own security risks

  Determines its risk tolerance or risk aversion

- **Risk Management (R)**

  Devises, implements, and maintains appropriate security to address its business requirements

ADMINISTRATIVE SAFEGUARDS (continued)

Security Management Process

- **Sanction Policy (R)**
- **Information System Activity Review (R)**

Sanctions must be clearly defined; Not just a generic statement in policies

Activity Review ("Internal Audit") Procedures for reviewing audit logs, access reports, and security incident tracking reports

Assigned Security Responsibility

Responsibility must rest with one individual to ensure accountability typically an Information Security Officer (ISO)

Large organizations may have site security coordinators working with the ISO

Smaller organizations may use the Privacy Official or outsource the ISO function

Workforce Security

Security standards extend to the members of a covered entity's workforce even if they work at home

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

Authorization controls to verify the identity of the workforce member

Types of background checks that will be conducted for workforce members

Termination – Collecting access control devices or changing door locks, etc.

Information Access Management

- **Isolating Healthcare Clearinghouse Function (R)**
- **Access authorization (A)**
- **Access Establishment and Modification (A)**

Isolating Healthcare Clearinghouse Function – New requirement

Requirement for "User-based, role-based, or context-based" was removed

Compliance with the Privacy Rule's "Minimum necessary" and JCAHO IM standards may drive role-based access controls

Security Awareness and Training

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

What is the difference between: Training, Education and Awareness?

What other information security content should be covered in workforce training?

Security awareness training is a critical activity, regardless of an organization's size.

ADMINISTRATIVE SAFEGUARDS (continued)

Security Incident Procedures

Goals:
Identify
Contain
Correct
Prevent

- **Response and Reporting (R)**

  Provides a way for users to report unusual occurrences in security or breaches to patient confidentiality

Contingency Plan

- **Data Backup Plan (R)**
- **Disaster Recovery Plan (R)**
- **Emergency Mode Operation Plan (R)**
- **Testing and Revision Procedure (A)**
- **Applications and Data Criticality Analysis (A)**

  Documented procedure for the secure, off-site storage and rotation of backups

  Work in conjunction with Data Owners to determine the organization's Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

Evaluation

Periodic review of technical controls and procedural review of the entity's security program

Non-Technical review –

- Self assessment or gap analysis
- Certification of systems
- Compliance documentation
- Audit logs and incident reports

Technical review –

- Vulnerability scans
- Testing of security controls

Business Associate Contracts and Other Arrangements

- **Written Contract or Other Arrangements (R)**

  Identify all business associates who receive or have access to electronic PHI

  Tie efforts with the Privacy initiative

  Leverage the opportunity to establish rules for remote access for vendors to limit downstream liability

PHYSICAL SAFEGUARDS

Facility Access Controls

- **Contingency Operations (A)**
- **Facility Security Plan (A)**
- **Access Control and Validation Procedures (A)**
- **Maintenance Records (A)**

To protect buildings, equipment, and media from natural and environmental hazards and unauthorized intrusions

Track maintenance records for door lock repairs or changes

Workstation Use

Workstation Security

Could address both in a single policy

Verify workstations are located to prevent unauthorized or casual viewing

Conduct a random audit of computer workstations to verify they have been updated with the latest version of virus definitions

Device and Media Controls

- **Disposal (R)**
- **Media Re-use (R)**
- **Accountability (A)**
- **Data backup and Storage (A)**

"Device" added to media controls to address things such as PDAs

Media Re-use is a new requirement; Sanitization of media (Overwriting the disk with random patterns of "1s" and "0s")

Importance of a Media Re-use Policy

There have been many news stories about people purchasing used computers and finding sensitive and confidential information stored on the hard disks. Some people have been able to retrieve names, addresses, medical information, Social Security Numbers, and credit card numbers.

Organizations must implement a strong media re-use policy to prevent these types of disclosures that could possibly lead to identity theft, "the fastest growing crime in America."

TECHNICAL SAFEGUARDS

Access Control

- Unique User Identification (R)
- Emergency Access Procedure (R)
- Automatic Logoff (A)
- Encryption and Decryption (A)

Unique UserID for accountability – *Most important for clinical applications*

Automatic logoff also permits an equivalent measure to restrict access

Encryption is an acceptable method of access control (data at rest)

Audit Controls

Use risk assessment and analysis to determine the extent of audit trails

Events that trigger an audit trail need to be jointly determined by the Data Owners, the Privacy and Security Officers

Check with vendors on audit capability

Store audit logs on a separate server

System administrators should not have access to the audit logs

Integrity

- **Mechanism to Authenticate Electronic PHI (A)**

Document any integrity controls that will be employed especially for transmissions outside of the internal network to ensure the validity of the data being sent or the sender of the data

Person or Entity Authentication

Person or entity authentication is primarily accomplished through UserID and passwords

The Security Rule does not specify any password requirements

Transmission Security

- **Integrity Controls (A)**
- **Encryption (A)**

"…When electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk."

Recognition that there is not a simple and interoperable solution to encrypting e-mail containing PHI

SECURITY: A BUSINESS PROCESS

Security: A Business Process

So how much security do you really need?

- You need a little more security than "the next guy"
- No such thing as 100% security
- "Reasonable and appropriate" measures need to be taken (due diligence)
- A balanced security approach provides due diligence without impeding health care

Three factors inhibit countermeasures:

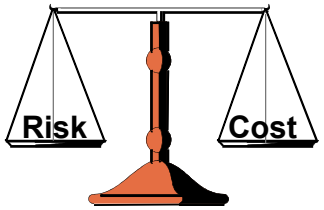
1. **Costs (Direct and indirect)**
2. **The "hassle factor" (Inconvenience)**
3. **May prevent legitimate access in an emergency**

Source: *For the Record: Protecting Electronic Health Information*

Balance

- Lack of adequate security results in the potential unauthorized access to confidential information.
- Too much security may hinder health care.

The goal is to reduce (not eliminate) risks to an acceptable level based upon an organization's "risk tolerance."



RESOURCES

- ISO 17799:2000, Code of Practice for Information Security Management
- NIST Special Publication 800 series:

  http://csrc.nist.gov/publications/nistpubs/index.html
- Handbook for HIPAA Security Implementation by Margret Amatayakul, Steve Lazarus, Tom Walsh, and Carolyn Hartley, which is being published by the American Medical Association in October 2003.
- "Best Practices for Compliance with the Final Security Rule" by Tom Walsh, published by HIMSS in the Journal of Healthcare Information Management, Volume 17, Number 3, Summer 2003

CONCLUSION

- The Security Rule requires covered entities to apply reasonable and appropriate safeguards and controls to protect electronic protected health information (ePHI)
- Whether required or addressable, the appropriate safeguards should be based upon an organization's risk analysis and best practices

The Final HIPAA Security Standards (February 2003)

ADMINISTRATIVE SAFEGUARDS §164.308			
Standards	**Section**	**Implementation Specifications**	
Security Management Process	164.308(a)(1)	Risk Analysis Risk Management Sanction Policy Information System Activity Review	R R R R
Assigned Security Responsibility	164.308(a)(2)		R
Workforce Security	164.308(a)(3)	Authorization and/or Supervision Workforce Clearance Procedure Termination Procedures	A A A
Information Access Management	164.308(a)(4)	Isolating Healthcare Clearinghouse Function Access Authorization Access Establishment and Modification	R A A
Security Awareness and Training	164.308(a)(5)	Security Reminders Protection from Malicious Software Log-in Monitoring Password Management	A A A A
Security Incident Procedures	164.308(a)(6)	Response and Reporting	R
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	R R R A A
Evaluation	164.308(a)(8)		R
Business Associate Contracts And Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangements	R
PHYSICAL SAFEGUARDS §164.310			
Standards	**Section**	**Implementation Specifications**	
Facility Access Controls	164.310(a)(1)	Contingency Operations Facility Security Plan Access Control & Validation Procedures Maintenance Records	A A A A
Workstation Use	164.310(b)		R
Workstation Security	164.310(c)		R
Device and Media Controls	164.310(d)(1)	Disposal Media Re-use Accountability Data Backup and Storage	R R A A
TECHNICAL SAFEGUARDS §164.312			
Standards	**Section**	**Implementation Specifications**	
Access Control	164.312(a)(1)	Unique User Identification Emergency Access Procedure Automatic Logoff Encryption and Decryption	R R A A
Audit Controls	164.312(b)		R
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI	A
Person or Entity Authentication	164.312(d)		R
Transmission Security	164.312(e)(1)	Integrity Controls Encryption	A A
ORGANIZATIONAL REQUIREMENTS §164.314			
POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS §164.316			

Legend: **R = Required – A = Addressable**