

# Reality vs. Hype: Risk-based Security Planning and Implementation

**Nebraska SNIP**

**November 21, 2003**

**Tom Walsh, CISSP**

**Tom Walsh  
Consulting, LLC**



---

Workshop materials created by Tom Walsh Consulting, LLC

Phone: 913-696-1573 ♦ e-mail: [twalshconsulting@aol.com](mailto:twalshconsulting@aol.com)

## Reality vs. Hype

**Q: What are the genuine risks to healthcare information systems?**

**Q: How much security does your organization really need to implement to comply with HIPAA?**

**Q: What will it cost to secure your systems?**

## Session Objectives

- Provide a high-level overview on the Security Rule
- Discuss a risk-based approach to compliance
- Present examples of "best practices" within healthcare information security
- Provide ideas on budgeting for security safeguards
- Review the importance of collaboration
- Provide resources for additional information

## Strategy – The Bigger Picture

Topic	HIPAA	The Bigger Picture
Needs to protect...	Electronic PHI	All information; financial, personnel, strategic, etc.
Attitude	"Is it in the rule?"	"Does it make good business sense?"
Compliance	April 2005	On-going
Penalties	\$100 per violation (Civil) \$50,000 - \$250,000 (Criminal)	\$150,000 for each program copied illegally Up to \$250,000 (Criminal)

*"Reasonable" was used 72 times in the Final Security Rule (Out of ≈50,000 words.)*

## HIPAA Security Standards

- 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.”

## Privacy versus Security

- Privacy Rule applies to PHI in paper, oral, and electronic form
- Parallels the Privacy Rule except:
  - Security Rule covers only electronic protected health information (ePHI)
- Security standards extend to the members of a covered entity’s workforce even if they work at home

*Workforce – Employees, contractors, temps, trainees, consultants and other persons under the direct control of the covered entity who have access to PHI in any medium*

## 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

## Risk Assessment and Analysis

**Risk = Threat x Vulnerability x Impact**

*If any one of the three equals zero, there is no risk*

### Each covered entity:

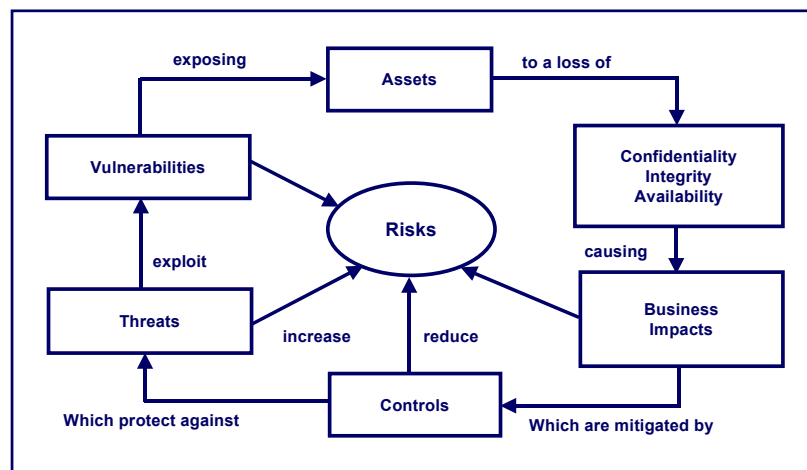
- Assess its own security risks
- Determine its risk tolerance or risk aversion
- Devise, implement, and maintain appropriate security to address its business requirements
- Document its security decisions

*Does not imply that organizations are given complete discretion to make their own rules.*

### Risk Assessment / Analysis

1. What needs to be protected?  
(Assets – Hardware, software, data, information)
2. What are the possible threats?  
(Acts of nature, Acts of man)
3. What are the vulnerabilities that can be exploited by the threats?
4. What is the probability or likelihood of a threat exploiting a vulnerability?
5. What is the impact, consequence, or loss to the organization?

*Risk assessment and analysis is like predicting the weather.*



**Risk should be handled in a cost-effective manner relative to the value of the asset. The analysis will determine if risks will be:**

- Mitigated/Reduced (Applying controls);
- Transferred (Insuring against a loss); or
- Accepted (Doing nothing, but recognizing risk)

## Determining a “Risk Score”

**The higher the number, the greater your risks.**

Source: The OCTAVE<sup>SM</sup> Approach

Impact	H	3	6	9
	M	2	4	6
	L	1	2	3
		L	M	H
		Likelihood		

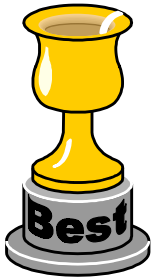
### Likelihood

(Source: NIST SP 800-30 Risk Management Guide for Information Technology Systems)

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

### Impact

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the high costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization’s mission, reputation, or interest.



## Best Practices

- Generally accepted principles and practices as determined by information security professionals
- Practices are typically derived from one or more principles
- They represent guidelines for developing or implementing information security
- Confidence in compliance

### Exercise

List some of the best practices in information security that you have either experienced or know about.

Also - How often should passwords be changed?

## Creating User Accounts

- Established on role-based access rules
- Unique UserID that is not based upon the user's name, department, telephone extension or employee number
- Systems prohibit concurrent/simultaneous access of the same UserID
- UserIDs are uniform across systems and platforms
- Policy governs the use of temporary, group-shared or generic UserIDs

## Managing User Accounts

- Managed by exception
- Access privileges are quickly changed if there is a change in the user's role (job transfer)
- IT is automatically notified by the HR/payroll system when a user's account should be inactivated because of employee resignation or termination
- Auto expiration of access for contractors, vendors, temps, residents, medical students

## Best Practices (continued)

### Creating Passwords

- IT department creates a random password
- The password is delivered to the user in a sealed envelope after the user completes their mandatory training or new-hire orientation
- There are limitations and parameters controlling the type of password that users may select (reuse, length, composition, etc.)
- Systems automatically force password changes especially at first logon

### Managing Passwords

- Users are trained on how to select a strong password
- Procedure for resetting users' passwords –
  - Help Desk verifies the identity of the caller using a pass phrase
  - Help Desk notifies the user's manager via e-mail about the user's password being reset

### Authentication

Three methods of authentication:

- Something you know  
Password, PIN, mother's maiden name, pass phrase
- Something you have  
ATM card, smart card, token, key, swipe card badge
- Something you are (biometric)  
Fingerprint, voice scan, iris scan, retina scan

*Combinations of any two = Two-factor authentication*

#### Can You Speak Geek?

Are there times when you struggle to understand your IT vendor or support staff, especially when they speak in technical jargon and acronyms? Well, here is a great resource on the Web to bookmark. TechWed's TechEncyclopedia ([www.techweb.com/encyclopedia](http://www.techweb.com/encyclopedia)) provides definitions and explanations of technical terms and acronyms. Next time you are not sure about a techie-term, write it down and look it up later on this Web site. While you may not speak geek, at least you'll have a better understanding of technical lingo.

## Security Controls - Prevention

- Policies, procedures, plans, etc.
- Training
- Workforce background checks
- Privacy or anti-glare screens
- Uninterruptible Power Source (UPS)
- Access controls
- Anti-virus software
- Fire proof media safe (for backups)
- Encryption software

## Security Controls – Detection

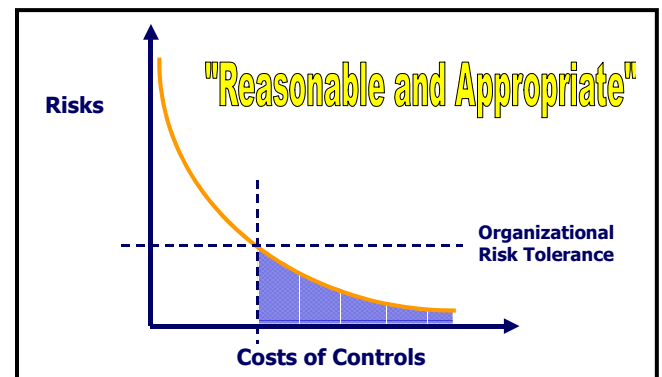
- Auditing
- Monitoring and alarms
- Example: Intrusion Detection Systems
- Surveillance cameras
- Door alarms
- Password cracking programs
- Vulnerability scanners

## Selecting Security Controls

- Current technology environment
- Risks associated with identified threats and vulnerabilities
- Future infrastructure plans
- Impact and organizational culture
- Budget

### Other factors to consider:

- “Low hanging fruit”
- Balance between security controls and the ease of use
- Balance between cost of the security control and the value of the information systems and data
- Diminishing returns on controls



## Security Controls

### Finding the “Right” Security Control

- Studies conducted by research firms (Example: Gartner Group)
- Buyer’s guide from information security trade journals
- Professional organizations
- Referrals from other organizations
- Collaboration

### **Budgeting for Security**

- Contingency and disaster recovery planning or support
- Audit controls (may require system upgrades or an additional server for storing and processing audit data.)
- Device and media controls
- Vulnerability scanning tools
- Encryption for secure transmission of ePHI

*Security is an investment, not an expense.*

### **Forces Working Against Us**

#### ***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)*

### **Collaboration**

- Sharing ideas saves time and money by
- Influencing and leveraging others
- Some (Security) opportunities include:
  - Establishing standards for secure transmission of ePHI (Encryption)
  - Disaster Recovery – Shared off-site facility; storage of off-site backups
  - Shared security officer (smaller facilities)
  - Authentication of identity
  - Policies and procedures
- May work with some of the same:
  - Insurance companies and Clearinghouses
  - Doctors, residents, medical students
  - Emergency response personnel:
  - State agencies
  - Vendors:
  - Support services and suppliers

**The Final HIPAA Security Standards (February 2003)**

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

Legend: R = Required – A = Addressable