



HIPAA SECURITY RISK ANALYSIS

WEDI National Conference

May 18, 2004

Presented by:

Lesley Berkeyheiser, The Clayton Group

Andrew H. Melczer, Ph.D., ISMS



Presentation Overview

- ◆ Key Security Points Review
- ◆ Risk Analysis
- ◆ Case Study and Findings
- ◆ Questions

Information Security is ...

◆ Assurance of

– Confidentiality

- the info is accessible only by authorized people and processes

– Integrity

- the info hasn't been inappropriately altered/destroyed

– Availability

- the info is there when needed

protected information (in any form)



Flexible & Scalable

- ◆ Each organization's security program should be based on *that* organization's risks and threats
- ◆ Security "solutions" should be based on circumstances such as: size, complexity, and capabilities – Scalability discussed later
- ◆ Security controls should be proportionate to risks and threats
 - Don't build a \$5,000 fence for a \$3,000 horse



Security is Forever

- ◆ Security made up of processes – not just a project, not just a product
- ◆ Cycle: prevent, detect, and respond
- ◆ Security dynamic, ever-changing
- ◆ Security requires ongoing monitoring
- ◆ Monitor (audit) compliance; monitor risks and threats
- ◆ Address new and new-found risks and threats

Standards

- ◆ Three categories of standards in rule:
 - Administrative
 - Physical
 - Technical
- ◆ All standards are required
- ◆ Some standards have no implementation specifications and stand on their own
- ◆ Some implementation specifications are required and some are addressable



Addressable

- ◆ **ADDRESSABLE DOES NOT MEAN OPTIONAL**
- ◆ There are no optional specifications
- ◆ All addressable items must be addressed based on an entity's risk analysis
- ◆ All decisions about addressable items must be documented

Addressable

- ◆ If an *implementation specification* is addressable, a covered entity may:
 - Implement, if reasonable and appropriate
 - Implement an equivalent measure, if reasonable and appropriate
 - Not implement – and document decision
- ◆ All actions and decisions must be based on sound, documented reasoning



Scalability

- ◆ HIPAA is “scalable”
- ◆ What you have to do depends on
 - Size
 - Resources
 - Technological sophistication
 - Circumstances
- ◆ The bigger you are, the more you must do
- ◆ Even if small, you must implement all HIPAA provisions



Scalability

- ◆ Makes HIPAA complex
 - No “standard” way to approach HIPAA
 - Depends on your situation
 - When someone says, “we must, so you must,” be careful
 - You may not have to implement in same manner as next covered entity
 - Lack of “standard” approach very confusing



ePHI

- ◆ Security rule applies to electronic protected health information (ePHI)
- ◆ AND ... Don't forget about paper and oral PHI: Privacy Rule contains “mini-security” rule
 - Covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information [§ 164.530(c)(1)]



ePHI

- ◆ So ... Must be taking reasonable steps now to ensure security of PHI
- ◆ Privacy Rule does not give guidance on how to protect paper and oral PHI
- ◆ And ... many of same standards in Security Rule should be considered to protect paper and oral PHI
- ◆ Remember: Without security you cannot ensure privacy

Risk Analysis

- ◆ Since organization's security approach based on its risk, first step to do risk analysis
- ◆ Be sure it's comprehensive
- ◆ *Be sure it's not limited to technical: Must also cover administrative and physical security* – what's in place and what's missing
- ◆ Be sure not limited to electronic info only



Risk Analysis

- ◆ Each covered entity must conduct accurate and thorough analysis of
 - Potential risks and vulnerabilities to
 - Confidentiality, integrity and availability (CIA) of ePHI
- ◆ ***Remember:*** While Security Rule applies only to ePHI, Privacy Rule applies to all PHI. Accordingly, risk analysis should not neglect paper-based and oral PHI



Risk Analysis

- ◆ Should be conducted before completing security policies and procedures
- ◆ Preamble states: “An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities” (Page 8346)

Risk Analysis

- ◆ Allows organization to
 - Evaluate areas of risk
 - Prioritize work effort
 - Allow time for investigation, selection and implementation of any necessary technical solutions
 - All in time to train workforce before compliance deadline – hopefully
- ◆ Will help identify existing policies and procedures that need to be documented and others that need to be modified



Timeline

- ◆ First: Conduct Risk Analysis
- ◆ Detail is scalable and reasonable based on size and complexity of CE
- ◆ May include simple review of Security Rule requirements or intense scrutiny of every possible information system using standard evaluation products (e.g., NIST)

Risk Analysis

- ◆ Once process completed, consider that security measures must remain current
- ◆ Some form of ongoing risk analysis must be repeated as necessary to allow for organization's adopted measures to be effective and current as organization's security environment changes over time



Assemble Your Team

- ◆ As with privacy, security must be implemented with a cross representation of expertise
- ◆ If CE is large enough to have multiple operational departments, risk analysis team should be multi-departmental
- ◆ Team may be small in small CE
 - Office manager, physician



Assemble Your Team

- ◆ If large, team might include
 - Those most familiar with CE's electronic systems (Security Officer and IT staff), responsible for compliance, responsible for operations
 - Privacy Officer, Regulatory/legal representation
 - Senior level official responsible for overall compliance with ability to focus staff and budget
 - Those who will have ongoing responsibility for training and for ownership of each policy and procedure



Getting Started

- ◆ First you need to understand Security Rule requirements
- ◆ Read rule and preamble
- ◆ Rule contains a lot of information and background
- ◆ Explains meaning and interpretation of many requirements



Getting Started

- ◆ Understand *your* unique security environment
- ◆ Get or develop schematic of *your* system configuration – if not too small a CE
- ◆ Talk with *your* information technology people about
 - How your system set up
 - How it is capable of being used
- ◆ Discuss recent events that may have compromised data CIA



Getting Started

- ◆ Discuss security topics at high level
- ◆ Use Final Rule as outline of discussion topics
- ◆ Start with Security Rule Chart
- ◆ Outlines rule requirements by major area, specification, and implementation specification



Getting Started

Administrative Safeguards

Standards	Sections	Implementation Specifications (R)= Required, (A)= Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)



Performing Risk Analysis

- ◆ Identify, evaluate and document *your* “assets” to define what *you* need to develop procedures to protect
- ◆ “Asset” is what organization values and wishes to protect in order to stay in business
- ◆ Assets can be defined in terms of quantity and quality

Performing Risk Analysis

- ◆ Assets may include:
 - Electronic confidential information
 - Paper confidential information
 - Organization's reputation
 - Other forms of data (e.g., financial)
 - Computer hardware and software
 - Buildings and real estate
 - Workforce members

Performing Risk Analysis

- ◆ Identify possible *threats* to your assets and the associated *risk level* of each threat
- ◆ “Threat” defined as “potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability”
- ◆ Consider threats to assets in the form of related losses as well

Performing Risk Analysis

- ◆ Threat can be
 - Computer or other process
 - An activity
 - An event
- ◆ Consider expected frequency of possible threats as well as “level of criticality,” i.e., how serious will damage be to CE if threat were carried out



Performing Risk Analysis

◆ Consider

- Natural threats like fires, earthquakes, floods, thunderstorms, hurricanes
- Accidental threats like contamination
- Those created by humans such as malicious threats like bomb, terrorist, theft, and vandalism
- Focus on internal threats, e.g., sharing passwords, inappropriate access to and disclosures of PHI by workforce

Performing Risk Analysis

- ◆ Losses can be categorized different ways
 - Direct losses such as those many businesses and lives experienced as a result of terrorist attacks on 9/11, medication errors
 - Delays or denials of services due to computer virus, power outages, other
 - Loss of reputation due to inappropriate disclosure of confidential information
 - Data alteration or destruction (loss of integrity)

Performing Risk Analysis

- ◆ Losses can be direct
 - Cost to replace computer, software
 - Cost to replace building
 - Legal costs to defend actions
- ◆ Losses can be indirect
 - Cost of personnel to work overtime to fix computer virus problem, make up interruption of business operations
 - “Intangible,” e.g., cost of embarrassment or loss of reputation



Consider Compliance Goal and Related Timelines

- ◆ Learn
- ◆ Conduct Risk Analysis
- ◆ Make Decisions
- ◆ Find Technical Solutions
- ◆ Implement
- ◆ Document
- ◆ Train



Case Study

- ◆ To determine level of detail a medium-sized practice needs to review to comprehensively assess its environment, potential threats and risks related to protecting PHI
- ◆ To assess number and types of resources needed to accomplish risk analysis and confirm estimated timeframes for completion



Small vs. Large Practice

- ◆ Security Regulations do allow for scalability
- ◆ Cost of compliance can be a factor
- ◆ Probability of risk can be a factor
- ◆ Required vs. Addressable
- ◆ Regulations technology neutral



Practice Description

- ◆ Specialty Practice
- ◆ 50+ FTE's
 - 8 physicians
 - 6 nurse practitioners
 - 36 support staff
 - 4 locations
 - Hospital affiliation



Security Environment

- ◆ Once “right” team established, environment needed to be assessed
 - Begin with access points; review ways ePHI utilized in practice
 - Enhanced communication between business and systems representatives
 - Validated capabilities of systems as compared to current ways systems being used



Assets and Threats

- ◆ Discussion of Assets
 - ePHI, paper patient charts, workforce, buildings, hardware software etc...
 - Focus on ePHI access points
- ◆ Discussion of Threats
 - Natural, human and environmental
 - (cold, frost snow/vandalism/chemical contamination)
 - Rate threats NA, Low, Medium and High

Review of Safeguards

- ◆ “Mix the ingredients together”...
 - Security environment findings
 - Assets, threats and determined risk level
 - Requirements and current safeguards
- ◆ in order to document risk analysis
- ◆ Prioritize Work Plan
- ◆ Begin Remediation



Case Study Findings

- ◆ Just because a practice is smaller doesn't mean the process is faster!
- ◆ Changes of titles and language...but process and accountability same as large organization
- ◆ Communication between IT and practice manager is key
- ◆ Threats are tricky
- ◆ Risk analysis allows for prioritization of work

Final Points

- ◆ Document
- ◆ Document
- ◆ Document every step of risk analysis
- ◆ Should there be a problem resulting in security breach, documentation will help demonstrate you did risk analysis and identified your risks and threats

Final Points

- ◆ You need to determine depth of review necessary for your organization
- ◆ If complex CE, may need to conduct more in depth risk analysis on certain business lines and/or entire information systems
- ◆ Consider whether industry guidelines should be considered
 - E.g., NIST, ISO 17799, FIPS 199, others



Final Points

- ◆ Small, non-complex CE, such as small practice, may simply “start with the chart” and use it as high level risk analysis outline
- ◆ Of course, basic review of small practices assets, potential threats and related losses needs to be completed and will assist in consideration of any changes necessary to meet Security Rule requirements

Final Points

- ◆ Go back and review your Privacy documentation...
 - Determine which security topics were already addressed
 - Determine level of risk assessment/analysis right for your organization
 - Use process (consider threats and abilities) to prioritize and...

Get to work!



WEDI/SNIP White Papers

- ◆ Many “hot topics”
- ◆ WEDI/SNIP prepared a number of white papers addressing these topics
- ◆ White papers available at no charge from web site
 - Go to snip.wedi.org
 - Go to Sub-workgroups, Security and Privacy, White Papers



QUESTIONS