



**WEDI**<sup>TM</sup>  
**SNIP**

Strategic National Implementation Process

# SECURITY PRIMER

**WEDI National Conference**

**May 17, 2004**

**Presented by:**

**Andrew H. Melczer, Ph.D., ISMS**

**Stanley Nachimson, CMS**



# Presentation Overview

- ◆ What is Security?
- ◆ Security Final Rule
  - Basics
  - Standards and Implementation Specifications
- ◆ Getting Started: Risk Assessment
- ◆ 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)



# Privacy versus Security

- ◆ Privacy relates to *what* must be kept confidential, e.g., medical information
- ◆ Security relates to *how* you keep it private, e.g., lock the door, use a firewall, limit access



# 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



# Security Final Rule



# Risk Analysis

- ◆ First step
- ◆ “Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity”



# 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)

# Timeline

- ◆ Second: Investigate and choose any technical solutions
- ◆ Identify departments accountable for new processes
- ◆ Complete policies and procedures – Iterative process

# Timeline

- ◆ Third: Implement new security measures
- ◆ Train workforce on new policies and procedures
- ◆ Need to allow adequate time to get from here to there
- ◆ Need adequate resources to get from here to there

# 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*

<b>Standards</b>	<b>Sections</b>	<b>Implementation Specifications (R)= Required, (A)= Addressable</b>	
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

# 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](http://snip.wedi.org)
  - Go to Sub-workgroups, Security and Privacy, White Papers



# QUESTIONS