Implementing the HIPAA Security Rule:
Special Publication 800-66

Safeguarding Health Information:
Building Assurance through HIPAA Security

A CMS – NIST Conference
May 19, 2009

Kevin Stine
Computer Security Division
National Institute of Standards and Technology
# NIST Publications Support the HIPAA Security Rule

<table>
<thead>
<tr>
<th>Some Security Rule Standards</th>
<th>Some Relevant NIST Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process (RA, RM)</td>
<td>SP 800-30, 800-37, 800-53</td>
</tr>
<tr>
<td>Access Control</td>
<td>SP 800-63</td>
</tr>
<tr>
<td>Security Awareness &amp; Training</td>
<td>SP 800-16, 800-50, 800-53</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>SP 800-34, 800-53</td>
</tr>
<tr>
<td>Evaluation</td>
<td>SP 800-37, 800-53, 800-53A</td>
</tr>
<tr>
<td>Device &amp; Media Controls</td>
<td>SP 800-53, 800-88, 800-111</td>
</tr>
<tr>
<td>Transmission Security (Encryption)</td>
<td>FIPS 140-2, SP 800-97, 800-113</td>
</tr>
</tbody>
</table>
What is Special Publication (SP) 800-66?

An Introductory Resource Guide for Implementing the HIPAA Security Rule

• Updated October 2008
• Intended as an aid to understanding security concepts discussed in the HIPAA Security Rule
• Directs readers to NIST publications relevant to topics addressed by the Security Rule
• Does not supplement, replace, or supersede the HIPAA Security Rule itself
Why We Updated 800-66?

• To reflect current NIST resources and publications

• To discuss the latest threats, vulnerabilities, and exposures, as well as the technologies used to combat them

• To propose methodologies covered entities may use to tackle specific Security Rule implementation challenges (ex, Risk Assessment, Contingency Planning)

• To set the stage, through security control mappings, for security automation of technical safeguards
NIST Risk Management Framework (RMF)

Step 1
CATEGORIZE Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT Security Controls
FIPS 200 / SP 800-53

Step 3
IMPLEMENT Security Controls
SP 800-70

Step 4
ASSESS Security Controls
SP 800-53A

Step 5
AUTHORIZE Information Systems
SP 800-37

Step 6
MONITOR Security State
SP 800-37 / 800-53A

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Risk Executive Function
Starting Point

Architecture Description
FEA Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Repeat as necessary

Security Life Cycle

Organizational View

Starting Point

Plan of Actions & Milestones

Security Assessment Report

Security Plan

Starting Point
Applying the Security Rule to the RMF

Monitor/Maintain
164.308(a)(8) – Evaluation
164.308(a)(1)(ii)(D) – Information System Activity Review

Authorization
164.308(a)(1)(ii)(B) – Risk Management

Evaluate
164.308(a)(8) – Evaluation

Identify EPHI
164.308(a)(1)(i) Security Management Process

Assess Risk and Apply Addressable Imp Specs
164.308(a)(1)(i) - Security Mgt Process
164.308(a)(1)(ii) (A) – Risk Analysis
(B) – Risk Management
164.316(b)(1) – Documentation
164.316(b)(2)(iii) - Updates

Implement
164.308(a)(1)(ii)(B) – Risk Management
Risk Assessment Guidelines

• Provide basic strategies to help covered entities identify and mitigate risks to acceptable levels

• Discuss the role of risk assessment in enterprise risk management

• Propose a methodology for conducting a risk assessment
Contingency Planning Guidelines

- Identify basic contingency planning principles and practices
- Discuss its role in a risk management process
- Discuss scope of different types of contingency plans
- Propose a process for developing and maintaining a contingency plan, and provide a sample template
Special Considerations

• Key Activities typically associated with each Security Rule standard

• Strategies and Considerations for Secure Remote Use and Access
## Setting the Stage for Automation: NIST Security Controls Support the Security Rule

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>164.312(a)(2)(iii)</td>
<td>Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.</td>
<td></td>
<td>AC-11, AC-12</td>
<td></td>
</tr>
<tr>
<td>164.312(a)(2)(iv)</td>
<td>Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information.</td>
<td></td>
<td>AC-3, SC-13</td>
<td></td>
</tr>
<tr>
<td>164.312(b)</td>
<td>Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
<td></td>
<td>AU-1, AU-2, AU-3, AU-4, AU-6, AU-7</td>
<td>NIST SP 800-12, NIST SP 800-14, NIST SP 800-42, NIST SP 800-53, NIST SP 800-55, NIST SP 800-92, NIST SP 800-115</td>
</tr>
<tr>
<td>164.312(c)(1)</td>
<td>Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.</td>
<td></td>
<td>CP-9, MP-2, MP-5, SC-8, SI-1, SI-7</td>
<td>NIST SP 800-12, NIST SP 800-14, NIST SP 800-53, NIST Draft SP 800-106, NIST Draft SP 800-107</td>
</tr>
<tr>
<td>164.312(c)(2)</td>
<td>Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</td>
<td></td>
<td>SC-8, SI-7</td>
<td></td>
</tr>
<tr>
<td>164.312(d)</td>
<td>Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.</td>
<td></td>
<td>IA-2, IA-3, IA-4</td>
<td>FIPS 201, NIST SP 800-12, NIST SP 800-14, NIST SP 800-53, NIST SP 800-63</td>
</tr>
</tbody>
</table>