Implementing the HIPAA Security Rule: Updates to Special Publication 800-66

HIPAA Security Rule Implementation and Assurance
January 16, 2008

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

<table>
<thead>
<tr>
<th>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 (Draft)</td>
</tr>
<tr>
<td>Device &amp; Media Controls</td>
<td>SP 800-88, 800-53, 800-34</td>
</tr>
<tr>
<td>Transmission Security (Encryption)</td>
<td>FIPS 140-2, SP 800-113, 800-97</td>
</tr>
</tbody>
</table>
What is Special Publication (SP) 800-66?

An *Introductory Resource Guide for Implementing the HIPAA Security Rule*

- Originally published in March 2005
- 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 Are We Updating 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 tackling specific Security Rule implementation challenges (ex, Risk Assessment, Contingency Planning)
What Can You Expect in the Update?

• General updates reflecting current NIST publications
• Introduction of the Risk Management Framework
• Guidelines on Risk Assessments and Contingency Planning
• Discussion on special considerations when applying the HIPAA Security Rule
• SP 800-53 security control mapping to Security Rule standards and implementation specifications, setting the stage for technical automation
NIST Risk Management Framework (RMF)

Starting Point
FIPS 199 / SP 800-60

CATEGORIZE
Information System

SELECT
Security Controls
FIPS 200 / SP 800-53

MONITOR
Security Controls
SP 800-37 / SP 800-53A

SP 800-37

AUTHORIZE
Information System
SP 800-53A

RISK MANAGEMENT
FRAMEWORK
Security Life Cycle

SUPPLEMENT
Security Controls
SP 800-37

SP 800-53 / SP 800-30

ASSESS
Security Controls
SP 800-53A

IMPLEMENT
Security Controls
SP 800-70

SP 800-18

DOCUMENT
Security Controls
Applying the Security Rule to the RMF

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

Identify EPHI and Required Imp Specs
164.308(a)(1)(i) Security Management Process

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

Evaluate
164.308(a)(8) – Evaluation

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

Document
164.316(b)(1) – Documentation
164.316(b)(2)(iii) - Updates

Assess Risk and Apply Addressable Imp Specs
164.308(a)(1)(ii)
(A) – Risk Analysis
(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 planning principles and practices for contingency plan development, and its function in a risk management process
• Discuss scope of different types of contingency plans
• Propose a process for developing and maintaining a contingency plan
Special Considerations

• Key Activities typically associated with each Security Rule standard

• Remote Access

• Removable Media Protections
SP 800-66 Publication Details

Estimated Publication Schedule

• Public Draft – January 2008
• Final – March 2008*

Where to find it

• NIST CSRC Website: http://csrc.nist.gov
Contact Information

Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Mailstop 8930
Gaithersburg, MD USA 20899-8930

Kevin Stine
Kevin.Stine@nist.gov

Matthew Scholl
Matthew.Scholl@nist.gov

CSD on the Web: http://csrc.nist.gov