



# HIPAA Security Rule Comparison

**Background Briefing**  
**Prepared for the**  
**HIT Policy Committee Tiger Team**  
**11/15/2011**



# What Are Security Frameworks?

- Organized taxonomies of security controls
- Grouped into logically related families
- May be open standards or proprietary
- HIPAA Security Rule published prior to current versions of security frameworks in common use today.
- Today's common frameworks evolved from earlier efforts; rapid evolution in the 1990s.
- HIPAA SR has not evolved in step with others.

# Common Security Frameworks



- HIPAA Security Rule
- ISO 27001
- FISMA (Federal Information Security Management Act)
  - NIST SP 800-53
- PCI DSS
- CoBIT
- HITRUST
  - A synthesis of multiple frameworks

# Let's look at two...



## FISMA

- Public Law 107-347: E-Government Act of 2002
- Title III, *Federal Information Security Management Act of 2002*
- “... provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets”

## ISO 27001

- ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*
- Specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information management system (ISMS) within the context of the organization's overall business risks

# FISMA tasked NIST to...



- Among other things,
  - ... develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, ... [FISMA, Section 303, (a)(3)]
- This resulted in ...
  - **Standard:** Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems (March 2006)*
  - **Guideline:** Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems and Organizations*

# There are 17 Security Control Families specified in FIPS 200 and SP 800-53

- Access Control
- Audit and Accountability
- Awareness and Training
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Two additional control families (*Program Management* and *Privacy* [draft]) not named in FIPS 200 have been added to SP 800-53.

# Here's an example from SP 800-53...

## Access Control (AC) Family

- AC-1 Access Control Policy and Procedures
- AC-2 Account Management
- AC-3 Access Enforcement
- AC-4 Information Flow Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege
- AC-7 Unsuccessful Login Attempts
- AC-8 System Use Notification
- AC-9 Previous Logon (Access) Notification
- AC-10 Concurrent Session Control
- AC-11 Session Lock
- AC-14 Permitted Actions without Identification or Authentication
- AC-16 Security Attributes
- AC-17 Remote Access
- AC-18 Wireless Access
- AC-19 Access Control for Mobile Devices
- AC-20 Use of External Information Systems
- AC-21 User-Based Collaboration and Information Sharing
- AC-22 Publicly Accessible Content

### AC-1: Access Control Policy and Procedures

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization defined frequency*]:

- a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

### AC-11: Session Lock

Control: The information system:

- a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and
- b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

# How Do FISMA and ISO Map to HIPAA?

**HIPAA Security Rule**

**ISO 27001**

**FISMA (FIPS  
200/SP 800-53)**

# Let's Look at One Example...



## Risk Analysis

The control described in HIPAA maps well to ISO and FISMA.

### HIPAA Security Rule, 164.308(a)(1)(ii)(A)

**Risk Analysis (R):** 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.

### ISO 27001:

- A.6.2.1,** Identification of risks related to external parties
- A.7.2.1,** Classification guidelines
- A.10.2.3,** Managing changes to third party services
- A.12.6.1,** Control of technical vulnerabilities
- A.14.1.2,** Business continuity and risk assessment
- A.15.1.4,** Data protection and privacy of personal information

### FISMA / SP 800-53:

#### **RA-3: Risk Assessment**

Conduct an assessment of risk...

#### **RA-5: Vulnerability Scanning**

Scan for vulnerabilities in information systems and applications...

Analyze reports...

#### **PM-9: Risk Management Strategy**

Develop and implement a comprehensive strategy to manage risk ...

#### **CM-4: Security Impact Analysis**

Analyze changes to systems to determine potential security impacts to information...



# Implications

- HIPAA Security Rules specifies that a risk analysis be done. This is consistent with other security frameworks.
- If the risk analysis is performed, the system will receive a similar level of protection/oversight as systems that conform to other frameworks.
  - Good practice is maintained.

# Let's Look at Another Example...



## Boundary Protections

The control described in ISO and FISMA is absent in HIPAA

### HIPAA Security Rule?

#### **FISMA / SP 800-53: SC-7 Boundary Protection**

The information system:

- a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
- b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

#### **ISO 27001:**

- A.10.6.1**, Network controls
- A.10.8.1**, Information exchange policies and procedures
- A.10.9.2**, Online transactions
- A.10.10.2**, Monitoring system use
- A.11.4.5**, Segregation in networks
- A.11.4.6**, Network connection control



# Implications

- HIPAA Security Rules does not require boundary controls.
- A system that conforms to the HIPAA SR can allow, for example, unmanaged or unmonitored interfaces between an EHR and the Internet, which may create a vulnerability that is not addressed.
  - Creates the possibility of undetected intrusion.



# Comparison Table

NIST SP 800-53 Revision 3 Security Control Family	Total Controls in Family	Total Controls Mapped to HSR	Percentage
Access Control (AC)	16	10	63%
Awareness & Training (AT)	4	4	100%
Audit & Accountability (AU)	12	9	75%
Certification, Accreditation, and Security Assessments (CA)	6	5	83%
Configuration Management (CM)	9	6	67%
Contingency Planning (CP)	9	9	100%
Identification & Authentication (IA)	8	8	100%
Incident Response (IR)	8	8	100%
Maintenance (MA)	6	5	83%
Media Protection (MP)	6	6	100%
Physical & Environmental Protection (PE)	18	10	56%
Planning (PL)	5	5	100%
Personnel Security (PS)	8	8	100%
Risk Assessment (RA)	4	4	100%
System & Services Acquisition (SA)	13	3	23%
System & Communications Protection (SC)	22	8	36%
System & Information Integrity (SI)	12	7	58%
Program Management (PM)	11	2	18%
<b>Summary</b>	<b>177</b>	<b>117</b>	<b>66%</b>

# Preliminary Conclusions of Co-Chairs



- Gaps exist between the HIPAA Security Rule and other commonly used security frameworks.
- The "framework" approach used in other contexts (FISMA, ISO, etc.) seems to allow for more frequent updating to keep up with innovation.
- A detailed analysis of the specific gaps - and coming up with recommendations to address specific security areas - is beyond the expertise of the Policy Committee.

# Draft Straw Recommendations (for discussion)



- Security policy for entities collecting, storing and sharing electronic health information needs to be more responsive to innovation and changes in the marketplace.
- Security policy needs to be flexible and scalable, given the difference in size and resources of entities covered by HHS rules and programs; at the same time, a more consistent baseline of security policies needs to be established and consistently implemented.



# Draft Recommendations (2)

- HHS should adopt a consistent, more dynamic process for regularly updating the security policies and technical standards for electronic health records and electronic health information exchange, deploying all of the policy tools within the Department's purview (HIPAA regulations and guidance, EHR certification, and where appropriate, conditions on federal funding programs like the meaningful use incentive program and HIE grants).
- HHS should begin by evaluating this gap analysis in more detail, with the goal of closing the gaps within a reasonable period of time. [specify time?]