



# Privacy and Security Tiger Team Meeting

**Recommendations regarding a framework of security protections for EHRs**

December 7, 2011

# Tiger Team Members

---

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, SAIC
- **Dan Callahan**, Social Security Administration
- **Neil Calman**, Institute for Family Health
- **Carol Diamond**, Markle Foundation
- **Judy Faulkner**, Epic
- **Leslie Francis**, University of Utah; NCVHS
- **Gayle Harrell**, Consumer Representative/Florida
- **John Houston**, University of Pittsburgh Medical Center
- **Alice Leiter**, National Partnership for Women & Families
- **David McCallie**, Cerner Corp.
- **Wes Rishel**, Gartner
- **Latanya Sweeney**, Carnegie Mellon University
- **Micky Tripathi**, Massachusetts eHealth Collaborative
  
- **Joy Pritts**, ONC
- **Deborah Lafky**, OCR
- **Kevin Stine**, NIST
- **Verne Rinker**, OCR

# Goal of Today's Discussion

---

- Briefly describe security rule “gap analysis” performed by ONC and NIST comparing the HIPAA security rule with other common information security frameworks
- Present recommendations on EHR security

# Background

- ONC staff, with the assistance of NIST, performed an analysis comparing the HIPAA Security Rule to other commonly used security frameworks.
  - Essentially this involved mapping the requirements and addressable specifications in the HIPAA Security Rule to the security controls in other frameworks

# 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; there was rapid evolution in the 1990s.
- In the view of the ONC and NIST staff performing this work, the HIPAA Security Rule 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
- ONC focused in particular looked at ISO 27001 and FISMA

# Overall results of FISMA analysis - 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>

## This analysis was presented to the Tiger Team

- ONC/NIST have determined that gaps exist between the HIPAA Security Rule and other commonly used security frameworks like FISMA.
- A detailed analysis of the specific gaps - and coming up with recommendations to address specific security areas - is beyond the expertise of the Tiger Team and the Policy Committee.
- However, the Tiger Team did believe there were some high-level recommendations on security policy that were worth presenting to the Policy Committee.

# Recommendations (slide 1)

1. Security policy for entities collecting, storing and sharing electronic health information (both HIPAA covered entities and business associates) needs to be responsive to innovation and changes in the marketplace.
2. 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 solid baseline of security policies needs to be established and consistently implemented (e.g., there must be a floor of policies that apply to all).

Note - This is currently the general approach of the HIPAA Security Rule.

## Recommendations (2)

3. Providers need education and guidance on how to comply with security policy requirements.
  - a. The Office for Civil Rights is required by HITECH to issue annual guidance on compliance with the HIPAA Security Rule, and since enactment of HITECH in 2009 they have issued guidance on how to complete a security risk analysis. This guidance is helpful for all entities covered by HIPAA (in particular those needing to do a risk assessment to qualify for Stage 1 of meaningful use). It can also serve as a good foundation for the development of more guidance on policy and countermeasures (business practices) for effectively managing identified risks.
  - b. Guidance should provide specific examples of policies and measures providers can implement to counter identified risk.
  - c. It's not clear how many providers know of the existence of this guidance. HHS needs to better educate providers about these resources (for example, through the RECs, professional societies and direct mail).

## Recommendations (3)

---

4. HHS also should have a consistent and dynamic process for updating security policies and the rapid dissemination of new rules and guidance to all affected. HHS should begin by evaluating the gap analysis performed by ONC and NIST in more detail.