



THE NEXT EVOLUTION OF HIPAA SECURITY

Kirsten Ruzic Wild

Senior Consultant

April 22, 2009

EXPERIENCE. INTEGRITY. RESULTS.

HIPAA Security Rule

Rule Requirements:

- establish national *minimum* standards for the security of electronic health care information
- published February 2003, deadline April 21, 2005
- administrative, technical, and physical security procedures (18 **standards**)
- **implementation specifications** are either Required (14) or Addressable (22)



HIPAA Security Rule

Rule Goals:

- Comprehensive, scaleable and technologically neutral (flexible)
- Protect the confidentiality, availability and integrity of ePHI
- Assess *risks and vulnerabilities*
- Improve Medicare/Medicaid through increased effectiveness and efficiency



HIPAA Security Rule

Rule Goals:

- “Improve efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements to enable the electronic exchange of certain health information”
- 45 CFR Parts 160, 162, 164 – Final Rule



HIPAA Security Rule

Interpretation:

- Good Thing: Scaleable and flexible
- Bad Thing: Scaleable and flexible
- How do you know if you meet the standard?
- Are you *certain* you are compliant?



HIPAA Security Rule

Interpretation:

- Lack of standard
- Constantly changing technologies
- Complexity and variety of clinical applications
- Limited IT budgets
- No **CMS** enforcement or oversight (years)
- Interpretation?

Why bother?



HIPAA Security Enforcement

Office of Inspector General (OIG)

- March 2007
- Piedmont Hospital – Atlanta
- Non-specific findings: significant *vulnerabilities*
- Leaked checklist of 42 questions/documents



HIPAA Security Enforcement

Office of Inspector General (OIG)

- August 2007
- Audit of CMS “to evaluate the effectiveness of CMS’s oversight and enforcement of covered entities’ implementation”
- Ongoing audits of covered entities nationwide for next few months
- No findings released



Guidance

CMS

- Late 2007
- Office of eHealth Standards and Services (OEHS)
- CMS website – HIPAA Security Standard
- Sample document request list for audit
- First insight into federal interpretation
- Conducting on-site reviews since January 2008



OCR/CMS Auditing/Enforcement

CMS

- Mid 2008
- Audited Providence Health and Services
- In cooperation with OCR
- Failure to implement P&P to protect PHI
- Portable media
- First Resolution Agreement/CAP
- On OCR website
- Only CMS audit results released



OCR/CMS Auditing/Enforcement

Providence Audit:

- No civil monetary penalty for cooperating
- Audited by OCR and CMS jointly
- Complaint-triggered audit



OIG Guidance

Findings:

- Audit of CMS August 2007
- Results of audit released in October 2008
- 14 months
- Develop understanding of CE interpretation of flexible and scalable ???



OIG Guidance

Findings:

- No compliance reviews had been conducted in 2 years
- CMS had “not provided effective oversight or encouraged enforcement of the HIPAA Security Rule”
- CMS agreed to implement a formal audit process
- Defense: voluntary compliance and complaint-driven



CMS Enforcement

Active Enforcement:

- Enforcement Statistics – types of complaints
- 330 complaints/investigations per month – open and closed
- A single complaint can result in 2 violations ,etc.



CMS Enforcement

Enforcement Statistics – 3 largest number of complaints

- Information **Access** Management (*Administrative Standard 164.308(a)(4)(i)*)
- Access Control (*Technical Standard 164.312(a)(1)*)
- Security Awareness and Training (*Administrative Standard 164.308(a)(5)(i)*)



CMS Enforcement

HIPAA Complaint Examples

- Scenarios – shared passwords, patient information viewable on provider's website meant for patient self-scheduling
- Both closed after CAPS



Other Governmental Agencies

- OESS HIPAA Security Series
- U.S. Department of Commerce - National Institute of Standards and Technology (NIST)



Conclusions

- Uncoordinated guidance, interpretation and enforcement
- Info on a variety of government websites OIG, CMS, OESS, OCR, Dept of Commerce
- Not easy to find
- Where do you go from here?



HIPAA Collaborative of Wisconsin

- HIPAA COW
- Security Networking Group
- **Benchmarking Survey**
 - ✓ March 2009
 - ✓ Goals: to provide benchmarking data to help organizations across the State determine their level of compliance with the regulations in preparation for a federal audit



HIPAA COW

Benchmarking Survey:

- 56 questions
- 10 categories
 - ✓ PHI encryption, auditing, e-mail retention, password management, portable media, etc
- Average of 76 responses to each question
- Respondents include: acute care hospitals, clinics/physician groups, long-term care facilities, payers, and integrated health care delivery networks
- From <200 to >2000 employees



HIPAA COW: Benchmarking Survey Results:

Encryption:

- 54% of respondents indicated they encrypt e-mail (46% do not currently encrypt e-mail)
- 34% of respondents indicated they encrypt laptop hard drives (66% do not)
- 26% indicated they do not encrypt any devices or data transmission



HIPAA COW: Benchmarking Survey Results:

Password Requirements:

- 92% of respondents said they did have minimum password length requirements
- Of those who do require a minimum length, 84% require 6-8 characters
- 47% require network passwords to be changed every 30-90 days
- *Doesn't appear there is a lot of variation...most of us agree on standard*



HIPAA COW: Benchmarking Survey Results:

Portable Media:

- 49% of respondents indicated they allow PHI to be loaded on portable media (51% responded their organization does not allow PHI to be loaded on portable media)
- Of those who allow PHI to be loaded on portable media, 32% *have no requirements to password protect or encrypt the data*



HIPAA COW: Benchmarking Survey Results:

Portable Media:

- 79% are not confident *they even know* the number of portable devices used by employees. (So how do you protect what you don't even know about?)
- *This is likely one of the greatest, if not **the** greatest, risk/s for covered entities.*



HIPAA COW - OIG Auditors

Findings – Administrative

- Contingency plan incomplete
- Backup tapes at risk
- No backup tape catalogs



HIPAA COW - OIG Auditors

Findings - Technical

- Access Control Vulnerabilities
 - ✓ Wireless – No encryption or WEP
 - ✓ Adequate security settings not applied
 - ✓ User access levels not reviewed
 - ✓ Inactive accounts not disabled or locked
 - ✓ User accounts inactive for excessive periods
- Audit Control Vulnerabilities
 - ✓ Server settings for audit logging disabled



HIPAA COW - OIG Auditors

Findings - Technical

- Integrity Control Vulnerabilities
 - ✓ Unsupported OS by Manufacturer
 - ✓ Inconsistently applied security patches
 - ✓ Computers lacked current antivirus update
 - ✓ Personal computers and servers lacked current service packs
- Transmission Security Vulnerability
 - ✓ Unencrypted sensitive information on compact discs



HIPAA COW - OIG Auditors

Findings – Physical

- Physical Safeguard Vulnerabilities
 - ✓ Uncontrolled access to EPHI
 - ✓ Deactivated alarm on emergency door
- Equipment Control Vulnerabilities
 - ✓ No computer equipment inventory
 - ✓ No password protection for computers on portable carts
 - ✓ No written plan for media disposal



Conclusions

- Most significant risk: passive loss of data due to own inaction; *failure to properly implement all the regulations resulting in non-compliant activity by authorized user*
- Increased government scrutiny
- Target for audits still complaint-driven
- Collaboration between OCR and CMS



Action Plan

- Risk Assessment – identify vulnerabilities
 - ✓ Access management and access control
 - ✓ Remote access and portable media
- Documentation
 - ✓ P&P – access management/control, training
 - ✓ Rationale for *addressable* not *required* specifications
 - ✓ CMS document and interview request list – completed?



Action Plan

- Training

- ✓ Last training 2005? General Orientation?
- ✓ Based on P&P
- ✓ Greatest risk areas
- ✓ Remote access and portable media – attestation
- ✓ Scenarios and staff meetings



Action Plan

- Training & Attitudes

“They just don’t get it”

- Change Process/Technology Adoption Lifecycle
- Everett Rogers “Diffusion of Innovations” 1957 - defined 5 categories of Adopters or individual responses to change



Action Plan

5 categories of Adopters:

- Innovators: eager to try new ideas, adventuresome, prepared for setbacks and not discouraged, launch new ideas
- Early Adopters: high degree of opinion leadership; social leaders
- Early Majority: cautious toward change, rarely lead change efforts but willing to adopt new ideas



Action Plan

- Late Majority: view change with skepticism and caution, feel pressured to embrace change from others who have already adopted
- Laggards: very traditional and last to adopt, point of reference is the past, decisions are made in terms of what has been done in the previously, adoption of change lags behind their awareness and knowledge level



Action Plan

- **What** do you **do** with the Laggards?
- Laggards do eventually get there but processes must be well-established
- Identify personality types in response to change
- Adult education principles



Action Plan

- Discipline – training without enforcement ?????
- Remember the OIG reprimanded CMS for lack of enforcement
- Serious consequences
- Organization at risk
- Best defense
- Why are we here?



American Recovery and Reinvestment Act (ARRA)

- HITECH and HIPAA – Incentives for establishment of infrastructure and standards
 - ✓ Privacy Advisor – each regional HHS office
 - ✓ National Coordinator for HIT (ONCHIT) – set policy, standards, specifications and criteria for HIT and EHR
 - ✓ Business Associates same as covered entities
 - ✓ Security/Data Breach Notification
 - ✓ Heightened enforcement
 - ✓ Accounting of Disclosures from EHR
 - ✓ Individual criminal liability



ARRA and HIPAA Security

- More than 30 additional guidances, reports, rules, standards, definitions yet to come
- Over next 5 years
- Many in next 6-18 months
- Continue to work on implementation
- Pay attention to upcoming changes and additions



Sinaiko Healthcare Consulting

- Conduct comprehensive Risk Assessments
- Interpretation of regulations
- Development and implementation of Training Programs
- Creation of or to revisions Policies and Procedures
- Perform audits
- Assist/support of governmental investigations



Evolution of HIPAA

Contact Info:

Kirsten Ruzic Wild

262-993-4747

310-551-5252

kirsten.wild@sinaiko.com

www.sinaiko.com

