HIPAA Security Compliance – An Industry Perspective

Susan A. Miller, J D
WEDI Security + Privacy Workgroup
Co-chair
Federal Security Environment

- HIPAA Security Rule
  - Contingency Plan
  - Logging and Auditing
- December 2006 Security Guidance
  - Mobile and wireless
- NIST Special Publications
  - Risk Assessment
  - HIPAA Security
- Breach and Breach Notification
  - Encryption
  - Data Destruction
- Additional HITECH Act Requirements
  - Enforcement
- Standards and Certification
- Red Flags
Federal Security Guidance Ideas

- WEDI SPWG: Small Practice Implementation White Paper
- Original OESS Security outlines
- NIST HI PAA Security Special Publications
Thank You!

Any Questions?

For additional information, please contact:

Sue Miller
TMSAM@aol.com
978-369-2092
HIPAA Security Compliance: Physician Practice Perspective

Safeguarding Health Information: Building Assurance Through HIPAA Security

OCR-NIST – May 12, 2010

Robert M. Tennant, MA
Senior Policy Advisor
Medical Group Management Association
rtennant@mgma.com
202-293-3450
The Medical Group Management Association

mission...

To continually improve the performance of medical group practice professionals and the organizations they represent

MGMA has

• 22,500 members...
• Who manage and lead 13,700 organizations
• With 275,000 physicians
• Providing about 40% of U.S. physician services
Current Environment

- Increasing numbers of practices are adopting EHRs
- HIEs are growing in number and are impacting practice data flow
- Data sharing for clinical purposes and P4P on the rise
- Patients are increasingly worried that sensitive health information might leak because of weak security
- Successful acceptance of EHRs and PHRs will require earning the public’s trust their PHI will be kept private and secure
- Health care lags significantly behind other industries in security
- Providers face unique security challenges and have limited abilities and resources
Where are Practice Risks?

- Loss of financial data (identity theft)
- Permanent loss of confidential information
- Temporary loss of medical records
- Unauthorized access to confidential information
- Loss of physical assets (i.e., computers, smartphones)
- Damage to practice reputation, patient confidence
- Business continuity
- Government enforcement
New HITECH Challenges

• Accounting for disclosures for treatment, payment, healthcare operations (practices with an EHR)
  – PHI in multiple locations
  – Collection
  – Usefulness to patient

• Breach notification
  – “Burden of proof”
  – Patient notification issues
  – HHS/Media alert

• Electronic copies of medical records

• Business associates as covered entities

• Sale of PHI/marketing

• Enforcement
Physician Practice To-Do List...

✓ Identify systems that have covered data

✓ Implement full Privacy and Security Rule compliance including risk assessment, policies, procedures, etc.

✓ Develop breach notification policy and plans— you need this for state laws and start logging breaches now

✓ Evaluate existing privacy and security policies and procedures and assess whether current administrative, technical and physical safeguards are sufficient to protect the privacy and security of PHI.

✓ Determine if currently encrypt or have the capability to encrypt PHI (the cost of encryption likely is less expensive than addressing a security breach)

✓ Review medical record retention and destruction policies to confirm that data is being destroyed properly

✓ Train... and retrain staff

✓ Don’t be in denial – willful neglect will cost you
Opportunities for NIST/OCR

• Additional “RFIs” to solicit opinions/perspectives from the industry
• Directly link Security with Privacy (especially breach)
• Directly link Security and Privacy with business continuity
• Create “readable” guidance/templates on critical issues and terms such as:
  – Encryption
  – Business associates
  – Minimum necessary
  – Limited data set
  – Privacy notice
• Expand/update and promote the 7-part “Security Series”
• Face-to-face educational sessions / focus groups at conferences
• National provider conference calls when new regulations / guidance released
• Solicited audits (similar to OSHA) / publish (anonymously) the results and recommended corrective actions (i.e., http://www.osha.gov/SLTC/hazardouswaste/osha.html)
Safeguarding Health Information: Building Assurance Through HIPAA Security
OCR-NIST – May 12, 2010

HIPAA Security Compliance: Health Information Management (HIM) Perspective

Dan Rode, MBA, CHPS, FHFMA
Vice President, Policy and Government Relations
AHIMA-HIM

82 year-old nonprofit professional association

7 professional credentials including privacy & security

57,000+ members/ 40 employer types/ 125 different functions in health information and informatics including: collection, abstraction, coding, reporting, transfer, storage, analysis, disbursement, and protection of health information

Association working in a variety of standards and best practice arenas including transactions terminologies and classifications, quality reporting, ISO, and confidentiality, privacy and security
HIM Current Issues -- HIPAA

Paper – hybrid – electronic records

Security Risk Assessment
  Budget
  Interface with IT hardware and software changes
  Lack of control (systems and disclosure) in larger institutions
  Vendor dependency

Logging and audit capacity

Patient access:
  For paper record/information
  “Portals”
  Limitations on “electronic requests”
HIM Current Issues – HIPAA (continued)

Extremely limited requests for accounting
Use of security varies – it may be in the system but it may not be turned on.
   Integration of systems
   Education by vendors
Understanding of security options and use is low.
Product capacity and demand ➔ ↔
Encryption anxiety
HIM Current Issues -- Transition

Certification dependency
Information (RFI) and Request (RFP)
Involvement and understanding of local health information exchange (HIE) activities
  Involvement and understanding of HIM functions and requirements
Policy maker understanding
New relationships and partnerships
Federal and state requirements – conflicts
Breach requirements – federal, state, and “risk.”
Legacy systems
Data integrity!
HIM Current Issues – ARRA-HITECH

Minimum Meaningful Use – product limitations
Maintaining security with data sequestering and individual data “privacy” requests
Working with business associates – data access issues
Involvement with patients and security, integrity, and accessibility requirements – understanding?
   Portal requirements and accessibility
Understanding of NIST standards
Use v Disclosure requirements and impact on security requirements and processes
Authentication anxiety!!!
Lack of common identifiers – integrity
Education
Resources and Contact

AHIMA General Webpage:  www.ahima.org
HITECH:  www.ahima.org/arra
Positions, comments, etc.:  www.ahima.org/advocacy

Dan Rode, MBA, CPHS, FHFMA
Vice President, Policy and Government Relations
American Health Information Management Association
1730 M Street, NW, Suite 502
Washington, DC 20036
Telephone:  (202) 659-9440
E-Mail:  dan.rode@ahima.org
HIMSS Survey Headlines

Despite changes in the privacy and security and landscape:

- Healthcare organizations have made relatively little change in the past year across a number of critical areas in the security environment.
- Risk assessments are not universal among responding organizations.
- While most organizations don’t have a plan in place to respond to a threat or security breach, many actively attempt to determine the cause of a breach at their organization.
Survey Headlines

• Organizations are widely using some technologies (audit logs and firewalls) but are not fully leveraging all technologies available to secure patient information

• Audit logs are widely used among the organizations represented in this survey
  – Data from firewalls, application logs and server logs are retained in the audit logs

• Organizations are still using manual capabilities to assess data in the audit logs
Survey Headlines

• Healthcare organizations widely share information with other organizations, such as government entities
  – This data sharing will increase in the future

• Healthcare organizations are also increasingly allowing patients and surrogates to access information
New Requirements under ARRA

• Breach Notification
  – Organizations are already notifying
  – ~60% report theft or loss of electronic devices

• Accounting of Disclosures
  – Regulation writing underway

• Sale and Marketing of PHI

• Coverage of Business Associates

• Enforcement/Penalties
Security Guidance Ideas

• Security Risk Assessment
  – Security Risk Assessment for Small Organizations
  – Data Flow Analysis
• Security Framework/Guidance
  – Deal with multiple statutory/regulatory requirements
• Accounting of Disclosures
• Breach Detection and Response
• Guidance for Business Associates
• Securing Wireless Devices