Healthcare Privacy and Security:

Breach prevention and mitigation/ Insuring for breach

Colin J. Zick
Foley Hoag LLP
(617) 832-1000
www.foleyhoag.com
www.securityprivacyandthelaw.com

Boston Bar Association
April 8, 2013

Breach Prevention

- Risk assessment
- Policies, procedures and training
- Self-audit and self-evaluation
- Feedback loop into policies, procedures and training

HHS OCR HIPAA Audit Program Protocol: What is it?

- The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits.
- The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.

HHS OCR HIPAA Audit Program Protocol: What does it cover?

- The audit protocol covers Privacy Rule requirements for:
  - (1) notice of privacy practices for PHI
  - (2) rights to request privacy protection for PHI
  - (3) access of individuals to PHI
  - (4) administrative requirements
  - (5) uses and disclosures of PHI
  - (6) amendment of PHI, and
  - (7) accounting of disclosures.
- The protocol covers Security Rule requirements for administrative, physical, and technical safeguards.
- The protocol also covers requirements for the Breach Notification Rule.

Key Issues Identified in OCR Audits

- Privacy:
  - Records of deceased
  - Personal representatives
  - Business associate agreements
  - Disclosures to courts and government entities
  - Verification of identity
- Security
  - Monitoring authorized users
  - Contingency planning
  - Authentication and integrity
  - Media reuse and destruction
  - Risk assessments
  - Granting or modifying user access

Administrative Safeguards: Security Management

- Where are the risks and vulnerabilities to our ePHI?
- What can we do to manage those risks?
- How will we sanction those who do not follow our policies that protect ePHI?
- How do we review our security records (e.g., logs, video, incident reports, etc.)
- Who is our security point person?

Administrative Safeguards: Workforce Security

- These are “addressable” and therefore can be adopted with flexibility to meet our unique needs:
  - What are our procedures for authorizing and supervising those with access to ePHI?
  - How do we approve people to access ePHI?
  - How do we terminate access to ePHI?

Administrative Safeguards: Information Access Management

- How to we keep our health plan information away from other, unrelated functions?
- What are our protocols for accessing health plan information at the computer terminal and program level?
- How do we modify that access?

Administrative Safeguards: Security Awareness and Training

- This is a very straightforward set of requirements:
  - What are our security reminders to personnel?
  - What do we have to protect our data against viruses, spyware, etc.?
  - How to we oversee who signs into the health plan computer systems?
  - How do we control and change computer passwords for systems with access to ePHI?

More Administrative Safeguards

- Security incident policies and procedures
- Contingency plans (data backup, disaster recovery, emergency operation, testing and revision, criticality analysis for applications and data)
- Periodic evaluation of security policies and procedures
- Review business associate agreements

Overview of Physical Safeguards

- Facility access controls (contingency plans, facility security plans, access control and validation, maintenance records)
- Workstation use policies and procedures
- Building, room, record, and workstation security to restrict access to authorized users
- Control on receipt and removal of hardware and media (disposal, use and reuse, inventory, backup and storage)

Physical Safeguards: Facility Access

- What are your policies and procedures regarding allowing authorized and limiting unauthorized access to ePHI and the areas it is housed?
- How do these policies and procedures identify those who are authorized to have access (e.g., by title, job function, name, etc.)?
- What are the physical access controls (e.g., locks, alarms, monitoring)?

Physical Safeguards: Contingency Operations

- What are the procedures in the event of a loss of power or other emergency?
- Do people with responsibility for the ePHI know about these procedures and how to implement them?

Physical Safeguards: Workstations, Device and Media Controls

- How do we specify what happens at workstations linked to ePHI?
- How do we dispose/reuse old computers and data sources (e.g., disks) that may have ePHI?
- Do people with responsibility for the ePHI know about these procedures and how to implement them?

Physical Safeguards: Facility Security/Access Control

- Where is ePHI kept and who has access to those places/systems?
  - These questions have to be asked and answered.
- Access control is a continuing process, as employees come and go regularly.

Technical Safeguards

- Access control (unique IDs, emergency access procedure, auto logoff, encryption)
- Audit controls
- Data integrity policies (authentication mechanisms)
- Person or entity authentication
- Transmission security (integrity and encryption)

Documentation Requirements

- Regulations require policies and procedures be documented (written record of any required actions).
- Retain documentation for 6 years.
- Make documentation available to those implementing procedures.
- Update documentation as necessary.

Breach Insurance Coverage: Leveraging Existing Policies

Depending on terms of policies, some claims and losses may be covered by the following policies:

- General Liability Coverage
- Professional Liability Coverage
- Lawyers' Professional Liability Coverage
- Errors and omissions

Stand-Alone Breach Insurance

- Still a developing area
- Limited history of evaluating risk, so premiums can vary widely
- Scope of coverage can vary widely
- Limits vary and can range from $25,000 to $25 million depending on the nature of the policy and business.
- What can be covered?
  - Crisis management services
  - Notification of breached parties
  - Credit/public records/fraud monitoring
  - Fraud remediation services

RESOURSES

- OCR: http://www.hhs.gov/ocr/privacy
- Audit protocol: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- My blog: http://www.securityprivacyandthelaw.com