Cybersecurity in the Health Care Sector: HIPAA Responsibilities from a Legal and Compliance Perspective

July 23, 2013

Gerry Hinkley, Pillsbury

Allen Briskin, Pillsbury

Overview

- Business associate obligations since the Omnibus Rule
- Developing an approach to HIPAA compliance – lessons from the OCR Pilot Audits

pillsbury

Business associate obligations Under Omnibus Final Rule

- Omnibus Rule conforms HIPAA regulations to HITECH Act changes
  - Before HITECH, BAs regulated through business associate contracts or agreements ("BACs")
  - After HITECH, BAs and subcontractors are regulated directly under HIPAA
    - Must comply with Security Rule (rule is flexible to accommodate small BAs)
    - Must comply with some of Privacy Rule and provisions of BAC

Business associates – expanded regulation

- Expanded definition of “business associate”
  - “Business associate” means one who, on behalf of a covered entity, creates, receives, maintains or transmits PHI
  - "Business associate" now also means "subcontractor of business associate“ who creates, receives, maintains or transmits PHI on behalf of a business associate
  - Status as BA based upon role and responsibilities, not upon who are the parties to the contract

pillsbury

Subcontractors of business associates

- Implications for subcontractor relationships
  - Contract between the covered entity's BA and that BA's subcontractor must satisfy the BAC requirements
  - Subcontractor of subcontractor is also a BA, and so on
  - As a result, HIPAA/HITECH obligations that apply to BAs also directly apply to subcontractors

Clarification of “who is a business associate”

- Rule clarifies definition of "business associate” -- included:
  - Patient Safety Organizations
  - Health information exchange organizations, e-prescribing gateways, covered entities' personal health record vendors (not all PHRs)
  - Data transmission providers that *require access to PHI on a routine basis*
- Not included – those who just provide transmission services, like digital couriers or “mere conduits”
  - However, those who store PHI, even if they don’t intend to actually view it, are BAs (NB: cloud model EHRs)

pillsbury

Business associates' use of protected health information

- Uses of PHI
  - BAs may use or disclose PHI only as permitted by BAC or required by law
  - BAs may not use or disclose PHI in manner that would violate Privacy Rule
  - Subcontractors subject to limits in initial CE-BA agreement – must pass along in subcontracts
  - BAs not making a permitted use or disclosure if not following minimum necessary rules
- BA does not comply if it knows of subcontractor's material noncompliance and does not take reasonable steps to cure the breach or, if such steps fail, to terminate the relationship

Consequences for business associates

- Secretary authorized to receive and investigate complaints against BAs (including subcontractors), and to take action regarding complaints and noncompliance
- BAs (incl. subs) required to maintain records and submit compliance reports to Secretary, cooperate in complaint investigations and compliance reviews, give Secretary access to information
- BAs (incl. subs) forbidden to intimidate, discriminate against, etc. those who make complaints, cooperate with regulators or oppose unlawful actions
- BAs (incl. subcontractors) subject to civil money penalties for HIPAA violations
- BA/subs remain liable under contract (BAC) to CE/BA

Business associate contracts – transition provisions

- Generally, compliance required 180 days Rule's effective date (3/26/13), which is 9/23/13
- Additional time allowed to enter into conforming business associate agreements (Limited Deemed Compliance Date)
  - If BACs comply with pre-Omnibus rule, parties have 1 additional year to bring their BACs into compliance with Omnibus Rule (9/22/14)
  - If BACs do not comply with pre-Omnibus rule (or no BAA exists), must enter into BACs that comply with Omnibus Rule by 9/23/13
  - Regardless of compliance deadlines, compliance with Omnibus Rule required when existing BACs renew or are modified

pillsbury

Business associate contracts – transition provisions

- BACs not otherwise modified or renewed prior to 9/22/14 must be brought into compliance by that date

pillsbury

Business associate contracts – new & changed provisions

- Definitions of “business associate” & “subcontractor”
- Business associate’s compliance with applicable provisions of the Security Rule
- Carrying out CE’s responsibilities in compliance with HIPAA
- BACs with subcontractors; obligations to seek cure of sub’s breach or terminate
- Assurances that subcontractor will appropriately safeguard PHI
- Assurances that subcontractor will comply with BA’s obligations to CE

Approach to HIPAA compliance – lessons learned from the OCR pilot audits

- Background on the pilot audits
- OCR's findings
- Adopting the Pilot Audit approach to internal HIPAA compliance
- Focus on the hot buttons
- Organize your documentation
- Utilize internal audit procedures to test compliance
- How to prepare for an eventual audit

What were the OCR pilot audits?

- OCR completed audits of 115 entities, including 61 providers, 47 Health Plans and 7clearinghouses
- OCR had 979 audit findings and observations, including 293 Privacy, 592 Security and 94 Breach Notification
- The Pilot Audits focused on:
  - The seven fundamental practices of the Privacy Rule
  - The administrative, physical and technical safeguards of the Security Rule
  - The requirements of the Breach Notification Rule

Audit findings

- HIPAA is not an organizational priority: lack of application of sufficient resources, incomplete implementation and sometimes complete disregard for HIPAA (30% didn't know they had HIPAA obligations)
- Failure to conduct regular risk assessments (70%)
- Minimum necessary not understood
- Security issues predominate over privacy issues
  - User access – authentication and limitations
  - Attention to encryption – either encrypt or explain why not
  - Media management – reuse and destruction

Adopt the pilot audit protocol for internal compliance

- Provide for a comprehensive assessment of policies, practices, systems, operations, infrastructure
- Determine whether routine operations implement policies that comply with legal requirements
- Targeted areas of high risk and frequent noncompliance
- Identify and correct critical weaknesses of compliance efforts

Hot buttons

- Current risk assessment (last three years)
- Response and reporting
- Awareness and training
- Access control – user activity monitoring
- Information access management
- Workstation security
- Business Associate contracts
- Minimum necessary
- Contingency planning
- De-identification

Documentation to study

- Organizational chart
- Policies and procedures, and specifically
  - Uses and disclosures
  - Breach notification
  - Complaints and sanctions
  - Incident response plans
  - Technical controls and information
  - Policies for physical safeguards

Documentation - 2

- Notice of privacy practices
- Network diagrams
- Training documentation
- Audit logs and other system generated information

Presenting material to internal audit in an organized manner

- Determine how best to present the documentation in an organized and responsive manner to tell the story about how your organization is committed to comply with the Privacy and Security Rules
- Trace the lifecycle of PHI at your organization
  - Know where high risk PHI exists
  - Is data encrypted and if not, how is it protected

Preparedness – assume you will be audited at some point

- Have a communication plan ready and engage senior leadership
- Prepare by performing self-assessments using the OCR Audit Protocols
- Conduct mock interviews of staff to prepare them for the Audit
- If compliance issues exist, focus on the biggest issues and /or those easier to fix
- Consider providing non-routine communications to serve as a refresher of key principles for all staff

Given what we know – a practical approach to getting ready

- Create a regulatory binder that contains the OCR and HHS guidance for the Audit and what/where/how list to access the required documents within your organization
  - The Audit Protocol found at http://ocrnotifications.hhs.gov/hipaa.html
  - List of contacts within your organization to assist in document retrieval for all aspects of the Audit, namely, privacy, security and breach notification
  - Recent risk assessment
  - Policies and procedures related to the Privacy and Security Rules
  - Notice of privacy practices
  - Monitoring/audit log reports

The purpose of this presentation is to inform and comment upon legal and regulatory developments in the health care industry. It is not intended, nor should it be used, as a substitute for specific legal advice inasmuch as legal counsel may only be given in response to inquiries regarding particular situations.

Contacts

Gerry Hinkley
Pillsbury Winthrop Shaw Pittman LLP
415.983.1135
gerry.hinkley@pillsburylaw.com

Allen Briskin
Pillsbury Winthrop Shaw Pittman LLP
415.983.1134
allen.briskin@pillsburylaw.com

pillsbury