Preparing for and Responding to an OCR HIPAA Audit

Carole Klove
Carole.Klove@ucsfmedctr.org

Gerry Hinkley
gerry.hinkley@pillsburylaw.com

SIXTH NATIONAL HIPAA SUMMIT WEST
October 10 - 12, 2012

Overview

- Background
- What to expect if you are audited
- How to prepare
- Subject areas to address
- How to organize your effort
- Lessons from the first wave of Audits

Background

- HITECH reflects the dissatisfaction of Congress with the lack of proactivity by Office of Civil Rights in enforcing HIPAA Title II – Health Information Privacy and Security
- Audit program objectives
  - Improve HIPAA Covered Entity compliance
  - Encourage assessment and development of security and privacy protections
  - Through Audit learnings, provide technical assistance to the industry
- Could lead to enforcement against Audit subjects, but this is considered unlikely
- KPMG selected to develop Audit protocols and conduct Audits

Audit protocol

- Provide for a comprehensive assessment of policies, practices, systems, operations, infrastructure
- Determine whether routine operations implement policies that comply with legal requirements
- Modular approach to allow targeted Audits to areas of high risk and frequent noncompliance
- Enable identification of critical weaknesses of Covered Entity's compliance efforts
- http://ocrnotifications.hhs.gov/hipaa.html

What we know about the Audit process

- The OCR HIPAA Audit program:
  - Processes
  - Controls
  - Policies
- The Audit focuses 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 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

The Audit timeline – the clock is ticking

- Notification Letter from the OCR triggers the Audit
- Documentation Due 10 days from the Notice
- Start of the Site Visit (30-90 days from the Notice)
- Period of analysis and questions
- Draft Audit Report (20-30 days from the end of the site visit)
- Comments on draft Audit Report due within 10 days from the Draft Audit Report)
- Final Audit Report (30 days after the Comment Period)

What - the documentation

- The request for documentation, includes, but is not limited to the following:
  - Audit logs and other system generated information
  - Organizational Chart
  - Policies and Procedures, and specifically
    - Uses and Disclosures
    - Breach Notification
    - Complaint and Sanctions

What - the documentation - 2

- Incident Response Plans
- Technical Controls and information
- Physical Safeguards
- Notice of Privacy Practices
- Network Diagrams
- Training Documentation

Where – retrieving the documentation

- Know in advance of an Audit where ALL the documentation is stored and it is key to know the format it can be retrieved and read
- Ensure that you know where system generated information, such as audit logs, exist and the lead time requested to extract the information
- Prepare by ensuring that you know where the complete, accurate and current documentation is located

How – presenting material in an organized manner

- Know how to interpret the system(s) generated information
- Trace the lifecycle of PHI at your organization
  - Know where high risk PHI exists
  - Is data encrypted and if not, how is it protected
- Think about how to best 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
- Prepare by performing self-assessments using the OCR Audit Protocols

Be Audit ready

- Have a communication plan ready and engage senior leadership
- Initially focus on the documentation request
- If compliance issues exist, focus on the biggest issues and /or those easier to fix
- Conduct mock interviews of staff to prepare them for the Audit
- Consider providing added communication to serve as a refresher of key principles for all staff
- It is a journey, not a destination, so be flexible and ready to demonstrate all the good work you have done!

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 regulatory binder should include the following items:
  - The Audit Protocol found at http://ocrnotifications.hhs.gov/hipaa.html
  - List of contracts 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

Audit site visit

- Interview leadership: CIO, privacy officer, legal counsel, medical records director
- Hands-on examination of physical features and operations of Covered Entity
- Determine consistency of processes to legal requirements
- Observe compliance efforts
- Notification that deficiencies could be the basis of compliance enforcement action
- Corrective actions designed to cure deficiencies can reduce potential penalties

Written findings

- Deficiencies
- Corrective actions in place
- Acknowledge best practices
- For each area examined
  - Condition
  - Criteria
  - Cause
  - Effect
  - Entity corrective actions

Lessons from the first wave of Audits

- HIPAA is not an organizational priority
- Small providers have significant compliance failures
- Failure to conduct regular risk assessments
- Minimum necessary not understood
- Security issues predominate over privacy issues
  - User access
  - Encryption
  - Media management – reuse and destruction

What, where, how and who

- In anticipation of an Audit, it is critical to know:
  - What documentation you have to support compliance with the Privacy and Security Rules;
  - Where the documentation resides;
  - How can you access the documentation and present it in a clear manner in response to the Audit; and,
  - Who can explain the documentation, including Audit findings, in a clear and comprehensive manner

Thank you!

Carole Klove
Director of Special Projects
UCSF Medical Center
Carole.Klove@ucsfmedctr.org

Gerry Hinkley
Partner
Pillsbury
gerry.hinkley@pillsburylaw.com

Preparing for and Responding to an OCR HIPAA Audit