2012 OCR HIPAA Privacy and Security Audit Program

HCCA Regional Annual Conference

Agenda

- Background
- Structure
- Audit Subject Selection
- Process & Timeline
- Results from Initial 20 Audits
- Next Steps
HITECH Act Impact

HITECH Act (of American Recovery and Reinvestment Act) of 2009

- Establishes breach notification requirements
- Establishes New Penalty Levels
- Establishes compliance requirements for business associates
- Extended Enforcement authority to State Attorneys General
- Mandates performance of privacy and security audits

Background

- The American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act, requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards
- To implement this mandate, OCR is piloting a program to perform up to 115 audits of covered entities to assess HIPAA privacy, security and breach notification performance
- Audits are conducted in two phases – initial audits to test the newly developed protocol and final pilot audits through December 2012
Program Objectives

Audits present a new opportunity to:

• Examine mechanisms for compliance
• Identify best practices
• Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
• Encourage renewed attention to compliance activities

Protocol Design & Program Performance Contract

• **Goal**: investigate and assess whether a CE is in compliance with Rules
• **Develop** in accordance with GAO auditing standards
• **Protocol**— comprehensive, modules to permit targeting of issues and entity types—designed for future use by OCR or others
• **Provide assessment** of policies, practices, operations and infrastructure
Who Will be Audited?

Every covered entity is eligible for an audit
For 2011-2012, OCR seeks to audit as wide a range of types and sizes of covered entities as possible which includes:

• Health plans of all types
• Health care clearinghouses
• Individual and organizational providers

Business Associates in later audit wave

Auditee Selection Criteria

OCR identified a pool of covered entities
Specific criteria includes but is not limited to:

• Public versus Private
• Entity’s size, e.g., level of revenues/assets, number of patients or employees, use of HIT
• Affiliation with other health care organizations
• Geographic location
• Type of entity and relationship to patient care
OCR Audits - Program Objectives

The objectives for the audit program are to improve covered entity compliance with the HIPAA privacy and security standards, through two approaches

• **Publicize Program**  OCR has widely publicized the audit program and anticipates publicizing the results of particular audits. OCR believes this will spur covered entities and their business associates to assess and calibrate their privacy and security protections.

• **Develop Industry Guidance**  In addition, OCR will post on its web site and broadly share leading practices gleaned through the audit process and guidance targeted to observed compliance challenges. Such technical assistance will assist those entities that are seeking information to frame their ongoing compliance efforts.

Timeline for the Audit Program

KPMG contract into effect June 2011; now standing up the program activities. Pilot audit program a three step process

1. **Working with KPMG to develop the draft audit protocols**
   
   *Completed November 2011*

2. **An initial round of audits tested the protocols. Results of field testing provided feedback for final protocol design.**
   
   *Field work completed March 1st*
   
   *Final protocol design completed April 2012*

3. **Rolling out the full range of audits and evaluation process.**
   
   *All audits will be completed by December, 2012*
How does the Audit Program Work?

- Entities selected for an audit will receive a notification letter from OCR and asked to provide documentation to the auditor.
- Every audit will include a site visit and result in an audit report.
- KPMG may recommend additional modifications to the protocol.
- KPMG will summarize findings & results, highlight consistent issues.
- Final report:
  - how the audit was conducted;
  - what the findings were and;
  - what actions the covered entity is taking in response to those findings.

What will be the Outcome of an Audit?

Audits are a type of review that serves more as a **compliance improvement tool** then an investigation of a particular violation that may lead to sanctions and penalties. An audit may uncover vulnerabilities and weaknesses that can be appropriately addressed through corrective action on the part of the entity.

It is possible that an audit could indicate serious compliance issues that may trigger a separate enforcement investigation by OCR.
**Breakdown of First 20 Auditees**

**Level 1 Entities**
- Large Provider / Health Plan
- Extensive use of HIT - complicated HIT enabled clinical/business work streams
- Revenues and or assets greater than $1 billion

**Level 2 Entities**
- Large regional hospital system (3-10 hospitals/region) / Regional Insurance Company
- Paper and HIT enabled work flows
- Revenues and or assets between $300 million and $1 billion

**Level 3 Entities**
- Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don’t adjudicate their claims
- Some but not extensive use of HIT – mostly paper based workflows
- Revenues between $50 Million and $300 million

**Level 4 Entities**
- Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)
- Little to no use of HIT – almost exclusively paper based workflows
- Revenues less than $50 million

---

**Overview of HIPAA Compliance Focus Areas**

**PRIVACY**
- Administrative Requirements
- Uses and Disclosures (U&D)
- Notice of Privacy Practices (NPP)
- Rights to Request Privacy Protection
- Access of Individuals to PHI

**Security**
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

**Breach Notification Requirements**
Initial 20 Findings Analysis Overview

Analysis of Findings by Rules

- Security: 65%
- Privacy: 26%
- Breach: 9%

Initial 20 Findings Analysis Privacy: Uses and Disclosures

Uses and Disclosures Analysis

- 4: Uses and Disclosures for Ensuring
- 2: Uses and Disclosures for Understanding
- 1: Others
Preliminary Observations From the Audits

- Policies and Procedures exist but some are outdated or not implemented
- HIPAA compliance programs were not a priority
- Small providers have broad failures across the Rules
- Larger entities continue to have security challenges
- Entities are not conducting regular Risk Assessments
- Privacy challenges are widely dispersed throughout the protocol - no clear trends by entity type or size
Next Steps to Consider

• Conduct a robust Assessment with an Annual or Bi-Annual reassessment for compliance
• Determine Lines of Business affected by HIPAA
• Consider internal employee health information in evaluation (Group Health Plan)
• Map/Flow PHI movement within your organization, as well as flows to/from third parties
• Perform Data discovery to find all of your PHI
• Establish effective technical safeguards over PHI (encryption, access management, restriction for required use only)

Conclusions & Final Thoughts

• Plan ahead for impact of HIPAA across the organization
  • Determine possible common responsibilities and oversight of IT, Information Security, and Internal Audit
  • Assess overlap between controls oversight and management
• Determine control and safeguard catalogue for HIPAA prior to remediation – know what you’re going after
• Engage impacted departments (IT, HR, Business, IA) early in the planning
• Assess your ability to combine HIPAA compliance activities with other compliance activities like PCI (Unified Compliance) to increase the effectiveness & efficiency of your compliance programs