2012 HIPAA Privacy and Security Audits

Linda Sanches
OCR Senior Advisor, Health Information Privacy
Lead, HIPAA Compliance Audits
Agenda

- Background
- Structure
- Audit Subject Selection
- Process & Timeline
- Initial 20 Auditees
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 Objective

• 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
Program Goal

To improve covered entity and business associate compliance with the HIPAA standards.

• Widely publicizing audit program & audit results will spur covered entities, business associates to assess and calibrate their privacy and security protections.

• OCR will share best 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.
# Audit Plan

<table>
<thead>
<tr>
<th>Description</th>
<th>Vendor</th>
<th>Status/Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit program development study</td>
<td>Booz Allen Hamilton</td>
<td>Closed 2010</td>
</tr>
<tr>
<td>Covered entity &amp; business associate identification and catalog</td>
<td>Booz Allen Hamilton</td>
<td>Closed 2012</td>
</tr>
<tr>
<td>Develop audit protocol and conduct audit</td>
<td>KPMG, Inc.</td>
<td>Open 2011-2012</td>
</tr>
<tr>
<td>Evaluation of audit program</td>
<td>TBD</td>
<td>To Be Awarded - Conclude in 2013</td>
</tr>
</tbody>
</table>
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
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 will 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 will recommend suggested 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.
What is a Performance Audit?

- Measure performance against established criteria
- Privacy, Security and Breach, “the Rules” were made auditable and measureable by developing performance criteria to execute these audits
- Used by regulators to understand how industry is complying with a set of regulations
- Conducted under GAGAS, Generally Accepted Government Auditing Standards, aka, Yellow Book Standards
- Allow for rendering an opinion of whether entity has key controls and processes to allow entity to maintain or achieve compliance with the Rules
- Not intended to be punitive, but rather measure compliance with regulations
Overview of HIPAA Audit Project
2011 - 2012

|------|-----|------|-----|-----|-----|-----|-----|-----|-----|------------|

Initial Protocol Development

Test of Initial 20 Audits

- Auditee Selection
- Auditee Notification
- Test of Protocol
- Period of Review/Adjustment of Protocols

-Audit Execution – Remaining Audits
- Protocol Updates As Needed
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
## First 20 Auditees by Entity Type

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Plans</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Healthcare Providers</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Healthcare Clearinghouses</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>5</td>
<td>6</td>
<td>3</td>
<td>6</td>
<td>20</td>
</tr>
</tbody>
</table>
# First 20 Plans and Providers

## Health Plans

<table>
<thead>
<tr>
<th>Health Plans</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Medicaid</td>
<td>1</td>
</tr>
<tr>
<td>SCHIP</td>
<td>1</td>
</tr>
<tr>
<td>Group Health</td>
<td>3</td>
</tr>
<tr>
<td>Health Insurance Issuer</td>
<td>3</td>
</tr>
</tbody>
</table>

## Health Care Providers

<table>
<thead>
<tr>
<th>Health Care Providers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allopathic &amp; Osteopathic Physicians</td>
<td>3</td>
</tr>
<tr>
<td>Hospitals</td>
<td>3</td>
</tr>
<tr>
<td>Laboratories</td>
<td>1</td>
</tr>
<tr>
<td>Dental</td>
<td>1</td>
</tr>
<tr>
<td>Nursing &amp; Custodial Care Facilities</td>
<td>1</td>
</tr>
<tr>
<td>Pharmacy</td>
<td>1</td>
</tr>
</tbody>
</table>
Initial 20 Findings Analysis Overview

Analysis of Findings by Rules

- Security: 65%
- Privacy: 26%
- Breach: 9%
Initial 20 Findings Analysis Overview

Analysis by Type of Covered Entity

- Health Plan: 16%
- Provider: 81%
- Clearinghouse: 4%
Initial 20 Findings Analysis Overview

Analysis of Finding by Tier

- Level 1: 11%
- Level 2: 8%
- Level 3: 15%
- Level 4: 66%
Initial 20 Findings Analysis
Privacy Issues

Privacy Audit Issues By Level of Entity

- Level 1: 3%
- Level 2: 4%
- Level 3: 16%
- Level 4: 77%
Initial 20 Findings Analysis

Privacy Issues

Privacy Audit Issues by Type of Entity

- 84% Provider
- 16% Health Plan
- 0% Clearinghouse
Initial 20 Findings Analysis Privacy: Uses and Disclosures

Uses and Disclosures Analysis

- Deceased Individuals: 4
- Personal representatives: 4
- Confidential communications: 2
- Business associate contracts: 4
- Permitted uses and disclosures: 3
- Consent for uses and disclosures: 1
- Authorization as Required for Internal Use: 1
- Limited uses and disclosures is required: 1
- Opportunity to Object: 1
- Uses and disclosures for research purposes: 1
- De-identification of PHI: 1
- Re-identification of PHI: 1
- Minimum Necessary Uses of PHI: 2
- Minimum Necessary Disclosures for Fundraising: 2
- Uses and Disclosures for Underwriting and Related Products: 1
- Verifications of the identity of those requesting PHI: 1
Initial 20 Findings Analysis
Privacy: Notice and Access

Notice of Privacy Practices for PHI – §164.520

Access of Individuals to PHI – §164.524
Initial Findings Analysis Privacy: Administrative Requirements

**Administrative Requirements – §164.530**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Training</td>
<td>3</td>
</tr>
<tr>
<td>Administrative, Technical and Physical Safeguards</td>
<td>2</td>
</tr>
<tr>
<td>Complaints to the Covered Entity</td>
<td>3</td>
</tr>
<tr>
<td>Sanctions of workforce regarding failure to comply with the Privacy policies and procedures</td>
<td>2</td>
</tr>
<tr>
<td>Mitigation of harmful effects that are known</td>
<td>3</td>
</tr>
<tr>
<td>Refraining from Intimidating or Retaliatory Acts</td>
<td>2</td>
</tr>
<tr>
<td>Policies and Procedures</td>
<td>4</td>
</tr>
</tbody>
</table>
Initial 20 Findings Analysis Security Issues

Security Audit Issues by Type of Entity

- Health Plan: 15%
- Provider: 79%
- Clearinghouse: 5%
Initial 20 Findings Analysis
Security Issues

Security Audit Issues by Level of Entity

- Level 1: 15%
- Level 2: 10%
- Level 3: 14%
- Level 4: 61%
Initial 20 Findings Security Issues

Security Audit Issues by Area of HIPAA Security Rule

- Administrative Safeguards – §164.308: 42.70%
- Physical Safeguards – §164.310: 16.76%
- Technical Safeguards – §164.312: 40.54%
Initial 20 Findings
Security Top Issues

<table>
<thead>
<tr>
<th>Area</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct Risk Assessment</td>
<td>17</td>
</tr>
<tr>
<td>Grant, Modify User Access</td>
<td>17</td>
</tr>
<tr>
<td>Incident Response</td>
<td>11</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>34</td>
</tr>
<tr>
<td>Media Reuse and Destruction</td>
<td>18</td>
</tr>
<tr>
<td>Encryption</td>
<td>10</td>
</tr>
<tr>
<td>User Activity Monitoring</td>
<td>46</td>
</tr>
<tr>
<td>Authentication / Integrity</td>
<td>19</td>
</tr>
<tr>
<td>Physical Access Controls</td>
<td>9</td>
</tr>
</tbody>
</table>
Preliminary Observations

• Policies and Procedures
• Priority HIPAA compliance programs
• Small providers
• Larger entities security challenges
• Conduct of Risk Assessments
• Managing third party risks
• Privacy challenges are widely dispersed throughout the protocol - no clear trends by entity type or size
Future of Audit

• All audits in pilot to end December 2012
• Findings will be used to look for trends
• Evaluation contract to conduct analysis of 2011 and 2012 activities
• Pilot experience and reports will feed into decisions re ongoing audit program
  • Structure, focus, size
Future of Audit

• TBD: Business Associates – more decisions
• BA Protocol Development
• Who to Audit – how to identify BAs
  • Who is a business associate? How to identify in the population?
  • Location; line of business; timeliness of information; subcontractors?
• What to Audit
  • Limited requirements for BAs
Non-Compliance Risks

• Loss of Contracts
• Criminal and Civil investigation
• Federal penalties, State fines
• Public Harm and Reputational Risk
• Legal Costs
• Cost of Notification
Next Steps to Consider

- Conduct a robust review & assessment
- Determine Lines of Business affected by HIPAA
- Map/Flow PHI movement within your organization, as well as flows to/from third parties
- Find all of your PHI
- See guidance available on OCR website