HIPAA Privacy, Security and Breach Notification Audits

Program Overview & Initial Analysis

Verne Rinker JD, MPH

2013 NIST / OCR Security Rule Conference
May 21-22, 2013
Program Mandate

HITECH Act, Section 13411 - Audits

- This section of The American Recovery and Reinvestment Act of 2009, 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.

Program Opportunity

- 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
## Multi-year 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 identification and cataloguing</td>
<td>Booz Allen Hamilton</td>
<td>Closed 2011</td>
</tr>
<tr>
<td>Develop audit protocol and conduct audits</td>
<td>KPMG, Inc.</td>
<td>Closed 2011-2012</td>
</tr>
<tr>
<td>Evaluation of audit program</td>
<td>PWC, LLP</td>
<td>Open Conclude in 2013</td>
</tr>
</tbody>
</table>
2011/2012 Implementation

Audit Protocol Design

• Created a comprehensive, flexible process for analyzing entity efforts to provide regulatory protections and individual rights

Resulting Audit Program

• Conducted 115 performance audits through December 2012 to identify findings in regard to adherence with standards. Two phases:
  • Initial 20 audits to test original audit protocol
  • Final 95 audits using modified audit protocol
What is a Performance Audit?

• An audit service conducted in accordance with GAGAS, Generally Accepted Government Auditing Standards (The Yellow Book)
• Provides findings, observations, or conclusions based on an evaluation of sufficient, appropriate evidence against established audit criteria
• Can include a limitless range of objectives driven by the needs of users
• Can entail objective assessments of a variety of attributes:
  – Program effectiveness, economy, and efficiency
  – Internal control
  – Compliance
  – Other questions of interest to management (e.g. value of assets, determination of pension benefits)
Who Can Be Audited?

Any Covered Entity
For 2011-2012, OCR sought wide range of types and sizes
- Health plans of all types
- Health care clearinghouses
- Individual and organizational providers

Any Business Associate
TBD after September 23, 2013 (HITECH Final Rule compliance date)
Breakdown of 2012 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 $300 million to $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 $50 Million to $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
# Auditees by Type & Size

<table>
<thead>
<tr>
<th></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>13</td>
<td>12</td>
<td>11</td>
<td>11</td>
<td>47</td>
</tr>
<tr>
<td>Health Care Providers</td>
<td>11</td>
<td>16</td>
<td>10</td>
<td>24</td>
<td>61</td>
</tr>
<tr>
<td>Health Care Clearinghouses</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>26</td>
<td>31</td>
<td>22</td>
<td>36</td>
<td>115</td>
</tr>
</tbody>
</table>
Audit Timeline

1 Business Day
- Notification Letter Sent to Covered Entities

20-60 Business Days
- Receiving and Reviewing Documentation and Planning the Audit Field Work

3-5 Business Days
- Onsite Field Work

10-20 * Business Days
- Draft Audit Report

10 Business Days
- Covered Entity Provides Management Responses

30-90 * Business Days
- Final Audit Report

Planning

Prep Work

Field Work

Post Field Work

* Duration varies based on several factors such as, the volume and complexity of findings noted
Audit Protocol—11 Modules

Breach Notification

Security
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Privacy
- Notice of Privacy Practices
- Rights to Request Privacy
- Protection of PHI
- Access of Individuals to PHI
- Administrative Requirements
- Uses and Disclosures of PHI
- Amendment of PHI
- Accounting of Disclosures
Established Criteria - Privacy, Security, and Breach Notification Rule criteria against which compliance is to be evaluated and assessed.

Audit Testing Procedures – Procedures executed to assess compliance with the criteria.

Workpaper Reference – Reference to workpaper documenting results of testing for the corresponding criteria.

Applicability - Whether or not the criteria/audit procedures are applicable for the Covered Entity.
The following slides walk through the protocol for § 164.508 – Uses & Disclosures. Process is repeated for each applicable section of the rule, listed in Appendices A & B.

1) Criteria

2) Audit Testing Procedures

3) W/P Ref.

4) Applicability
The audit team would execute this audit step through an interview with, for example, the Privacy Officer:

– Inquire of management as to whether a process exists to determine when authorization is required.
Audit Testing Procedure - Review

- The audit team would execute this audit step through review of documentation:
  - Obtain and review a sample of instances where authorization is required to determine if a valid authorization was obtained:
  - Evidence that an authorization was valid.
Potholes along the way

**Entity verification**
- Old addresses, no contacts
- CE’s that aren’t
- Nonresponsive

**Documents for review**
- Newly minted and not trained on (i.e., not implemented)

**Interaction and representation to KPMG**
- Intentional misrepresentation
- Disavowing staff statements
- GAGAS standards for trusted sources
Program Deliverables

Final Audit Reports
- Scope and methodology of the audits
- Findings and observations
- Covered Entity responses

Leading Practices
Exceptions Affect Audit Scope

• What did we audit? Varied by type of entity.
• Exceptions to certain requirements applied to several audited entities
  • 6 of the 7 clearinghouses asserted they only act as a business associate to other covered entities; in accordance with §164.500(b) few privacy procedures applied
  • 8 of the 47 health plans asserted they were fully insured group health plans, so only one privacy procedure applied.
  • 2 of the 61 providers and 4 of the 47 health plans asserted they do not create, receive or retain electronic Protected Health Information (ePHI), so security protocol was not executed.
Overall Findings & Observations

No findings or observations for 13 entities (11%)
- 2 Providers, 9 Health Plans, 2 Clearinghouses

Security accounted for 60% of the findings and observations—although only 28% of potential total.

Providers had a greater proportion of findings & observations (65%) than reflected by their proportion of the total set (53%).

Smaller, Level 4 entities struggle with all three areas
Audit Findings & Observations By Level

Audit Findings and Observations by Level of Entity

- Level 1: 41%
- Level 2: 20%
- Level 3: 19%
- Level 4: 20%
Proportional by Entity Type

AUDIT FINDINGS AND OBSERVATIONS BY TYPE OF COVERED ENTITY

- Provider: 65%
- Health Plan: 32%
- Clearinghouse: 3%
Proportional Findings by Rule

Audit Findings and Observations by Rule

- Security: 60%
- Privacy: 30%
- Breach: 10%
Element Exposure by Entity Type

Audit Findings and Observations Distribution

- Clearinghouse
- Health Plan
- Provider

Total Number of Audit Findings and Observations

0 1-5 6-10 11-20 >20

Number of Auditees

2 9 17 17 11

NIST / OCR May 22, 2013
Privacy Findings & Observations

PERCENTAGE OF FINDINGS AND OBSERVATIONS BY AREA OF FOCUS

- Notice of Privacy Practices for PHI: 20%
- Right to Request Privacy Protection for PHI: 2%
- Access of Individuals to PHI: 16%
- Administrative Requirements: 18%
- Uses and Disclosures of PHI: 44%
Privacy Results by Entity Type

Findings and Observations by Area and Type of Entity

- Providers
  - 43% Uses and Disclosures of PHI
  - 19% Administrative Requirements
  - 16% Access of Individuals to PHI
  - 2% Right to Request Privacy Protection for PHI
  - 20% Notice of Privacy Practices for PHI

- Health Plans
  - 43% Uses and Disclosures of PHI
  - 18% Administrative Requirements
  - 18% Access of Individuals to PHI
  - 1% Right to Request Privacy Protection for PHI
  - 20% Notice of Privacy Practices for PHI

- Clearinghouses
  - 75% Uses and Disclosures of PHI
  - 25% Administrative Requirements
Privacy Administrative Elements

Administrative Requirements Findings and Observations
Privacy -- Uses and Disclosures

Uses and Disclosures of PHI Findings and Observations

- Business Associates: 18%
- Identity Verification: 8%
- Minimum Necessary: 17%
- Authorizations: 11%
- Deceased Individuals: 9%
- Personal Representatives: 7%
- Judicial and Administrative Procedures: 4%
- Group Health Plan Requirements: 2%

NIST / OCR May 22, 2013 26
58 of 59 providers had at least one Security finding or observation.

No complete & accurate risk assessment in two thirds of entities:
- 47 of 59 providers,
- 20 out of 35 health plans and
- 2 out of 7 clearinghouses

Security addressable implementation specifications: Almost every entity had a finding or observation that could be met by fully implementing the addressable specification.
Security Elements

Percentage of Audit Findings and Observations by Area of Focus

- Risk Analysis: 14%
- Access Management: 14%
- Security Incident Procedures: 9%
- Contingency Planning and Backups: 12%
- Workstation Security: 14%
- Media Movement and Destruction: 7%
- Encryption: 8%
- Audit Controls and Monitoring: 14%
- Integrity Controls: 4%
Security by Entity Type

Total Audit Findings and Observations by Area of Focus and Entity Type

Area of Focus

Number of Audit Findings and Observations

- Risk Analysis
  - Clearinghouses: 3%
  - Health Plans: 29%
  - Providers: 68%
- Access Management
  - Clearinghouses: 4%
  - Health Plans: 26%
  - Providers: 71%
- Security Incident Procedures
  - Clearinghouses: 8%
  - Health Plans: 38%
  - Providers: 55%
- Contingency Planning and Backups
  - Clearinghouses: 74%
  - Health Plans: 1%
  - Providers: 7%
- Media Movement and Destruction
  - Clearinghouses: 1%
  - Health Plans: 25%
  - Providers: 67%
- Encryption
  - Clearinghouses: 6%
  - Health Plans: 6%
  - Providers: 69%
- Audit Controls and Monitoring
  - Clearinghouses: 31%
  - Health Plans: 29%
  - Providers: 65%
- Integrity Controls
  - Clearinghouses: 2%
  - Health Plans: 2%
  - Providers: 67%

NIST / OCR May 22, 2013
Breach Notification by Entity Type

Audit Findings and Observations by Requirement and Type of Entity

- **Notification to Individuals**: 58% (Providers), 42% (Clearinghouses), 8% (Health Plans)
- **Timeliness of Notification**: 57% (Providers), 43% (Clearinghouses), 8% (Health Plans)
- **Methods of Individuals Notification**: 63% (Providers), 37% (Clearinghouses), 0% (Health Plans)
- **Burden of Proof**: 52% (Providers), 44% (Clearinghouses), 4% (Health Plans)
Overall Cause Analysis

• For every finding and observation cited in the audit reports, audit identified a “Cause.”
• Most common across all entities: **entity unaware of the requirement.**
  • in 30% (289 of 980 findings and observations)
    • 39% (115 of 293) of Privacy
    • 27% (163 of 593) of Security
    • 12% (11) of Breach Notification
  • Most of these related to elements of the Rules that explicitly state what a covered entity must do to comply.
• Other causes noted included but not limited to:
  • Lack of application of sufficient resources
  • Incomplete implementation
  • Complete disregard
Cause Analysis – Top Elements

*Unaware of the Requirement*

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Notice of Privacy Practices;</td>
<td>• Risk Analysis;</td>
</tr>
<tr>
<td>• Access of Individuals;</td>
<td>• Media Movement and Disposal; and,</td>
</tr>
<tr>
<td>• Minimum Necessary; and,</td>
<td>• Audit Controls and Monitoring.</td>
</tr>
<tr>
<td>• Authorizations.</td>
<td></td>
</tr>
</tbody>
</table>
Next Steps for OCR

Formal Program Evaluation 2013

Internal analysis for follow up and next steps
• Creation of technical assistance based on results
• Determine where entity follow up is appropriate
• Identify leading practices

Revise Protocol to reflect Omnibus Rule

Ongoing program design and focus
• Business Associates
• Accreditation /Certification correlations?
New Provider Education Tools

- Patient Privacy: A Guide for Providers
  [Link](http://www.medscape.org/viewarticle/781892?src=ocr2)

- HIPAA and You: Building a Culture of Compliance
  [Link](http://www.medscape.org/viewarticle/762170?src=ocr2)

- Examining Compliance with the HIPAA Privacy Rule
  [Link](http://www.medscape.org/viewarticle/763251?src=ocr2)

These Medscape modules offer free Continuing Medical Education (CME) credits for physicians and Continuing Education (CE) credits for health care professionals.
Want More Information?

HIPAA Audit Webpage
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

OCR offers a wide range of helpful information about health information privacy including educational resources, FAQ’s, rule text and guidance for the Privacy, Security, and Breach Notification Rules
http://www.hhs.gov/ocr/privacy/