OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2

Linda Sanches, MPH
Senior Advisor, Health Information Privacy

HCCA Compliance Institute
March 31, 2014

Agenda

• Background
• Audit Phase 1
  • Design
  • 2012 Findings
  • Evaluation—major recommendations
• Audit Phase 2
  • Approach
  • Size
  • Timing
  • Focus
  • Entity selection
• Guidance
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

- OCR sought a comprehensive, flexible process for analyzing entity efforts to provide regulatory protections and individual rights.
- Identify best practices and uncover risks and vulnerabilities not identified through other enforcement tools
- Encourage consistent attention to compliance activities

Multi-year Phase 1

<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</td>
<td>Closed 2011-2012</td>
</tr>
<tr>
<td>Evaluation of audit program</td>
<td>PWC, LLP</td>
<td>Closed 2013</td>
</tr>
</tbody>
</table>
Phase 1 Building Blocks

- Comprehensive audit protocol and associated set of audit program work papers
- Databases of covered entities
- Methodology for entity selection
- Survey of entity attributes for audit planning
- Program evaluation
- Other foundational materials – Include templates for notification letters, final reports, document requests

Phase 1, Pilot 2011 -- 2012

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
Protocol—11 Modules

Breach Notification

Privacy

Security

• Administrative Safeguards
• Physical Safeguards
• Technical Safeguards

• 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

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

Proportional by Entity Type
Proportional Findings by Rule

Audit Findings and Observations by Rule

Privacy Findings & Observations

PERCENTAGE OF FINDINGS AND OBSERVATIONS BY AREA OF FOCUS
Security Results

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: most entities without a finding or observation met the standard 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 14%
- Contingency Planning and Backups 14%
- Workstation Security 14%
- Media Movement and Destruction 10%
- Encryption 7%
- Audit Controls and Monitoring 6%
- Integrity Controls 8%
- Compliance 9%
Breach Notification by Entity Type

Audit Findings and Observations by Requirement and Type of Entity

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>

### Objectives

- Communications
- Entity Selection
- Protocols

### PHASE ONE PROGRAM EVALUATION
Evaluation Objective

To determine if the implementation objectives of the audit plan and program were achieved. The assessment:

• Looked at the effectiveness of the protocol & auditing process in identifying compliance challenges;
• Methods applies included:
  • the review of audit data;
  • surveys of the audited covered entities; and,
  • interviews with audited covered entities
• Focused on what activities and resources facilitated the audit program, and understanding the barriers and/or problems that may have been encountered in the program.

Communication & Outreach Results

Audited covered entities generally felt positive about communications during the course of the audit:

• 90% agreed that communications prior to the onsite visit clearly explained the purpose of the audit
• 71% agreed that communications prior to the onsite visit clearly explained what would happen during the audit process
• 56% became aware of additional HIPAA regulations which apply to their organizations

However, 59% of responding covered entities were not aware of the audit program prior to receiving notification of selection. Most of these entities were also not aware that the audit protocol was available on the OCR website.
### Communication and Outreach

#### Recommendations

**Ongoing Publicity of the Audit Program**

- OCR should continue to widely publicize the audit program and overall results to prompt covered entities to proactively attempt to identify and correct potential compliance issues.
- For smaller entities, OCR may want to focus additional attention on forums and journals
- After each year of audits, OCR should evaluate areas of high risk and pervasive non-compliance and consider the creation and delivery of training on leading practices

---

**Selection Process**

#### Results

- Some surveyed audited entities indicated that the selection methodology should be published so that entities can understand the selection criteria.

#### Recommendation

- OCR should consider this request.
Recommendations:
Protocol Modifications

Consider updating the protocol to include test procedures that specifically address the review of specific types of documentation needed to meet the audit objective.

Add steps to guide auditors in tailoring the protocol to the specific covered entity type.

Revise the protocol to include the Omnibus Final Rule and reassess priority areas based on program audit results and industry feedback.

Selection of Requirements to Audit—
Recommendations

Implement a Risk-Based Approach

- A risk-based approach for applying audit protocols would allow OCR to determine areas of the Rules which require implementation of controls which, if not implemented effectively, pose the greatest risk to the protection of PHI.
- OCR should consider a multi-tiered audit approach which can be tailored based on entity type, area or a hybrid.
**Requested Documentation Results**

Survey results from responding covered entities regarding the documents and data requested of them:

- **87%**
  The documents and data requested were communicated clearly during the onsite visit

- **82%**
  The documents and data requested were clearly outlined in the original request

- **79%**
  The documents and data requested were sufficient for assessing compliance at their type of entity

*March 2014*

---

**Requested Documentation**

Results

- Survey comments and follow-up interviews also indicated some inconsistency in the document collection process:
  - Electronic vs. hard copy submission
  - Issues with the document repository causing resubmission
  - Misdirection of audit notification letters

*March 2014*
Timing and Staffing Levels
Recommendation--Implement a Centralized Staffing Tracker

Benefits:

- Captures historical data to identify the appropriate number of staff required for an audit
- More even distribution of man hours, which would likely decrease the range in time of testing
- Staff assigned based on the nature of the entity being reviewed
- Assign people with proper backgrounds
- Plan for and complete audits more easily
- Enhanced program oversight

Work Papers Recommendations

- **Use an Electronic Work Paper System (EWPS)**
- An EWPS system would provide a centralized mechanism for capturing documentation to support standards related to audit planning, fieldwork, reporting, and monitoring. This includes documentation for the following areas:

<table>
<thead>
<tr>
<th>Independence, both on an organizational and individual level</th>
<th>Professional judgment and competence (ex. auditor resumes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for conclusions (ex. Documentation provided by covered entities)</td>
<td>Planning (ex. agreed upon protocols, sampling methodologies)</td>
</tr>
<tr>
<td>Quality Control and Assurance</td>
<td>Clear supervisory review evidence</td>
</tr>
<tr>
<td>Audit work papers/narrative</td>
<td>Audit reports and referencing</td>
</tr>
</tbody>
</table>
Work Paper Recommendations

• Use Representative Sampling Methods
  • Representative sampling will help OCR to understand the degree to which an entity is compliant for a given focus area.
  • *Yellow Book section 6.64: random sampling* is the preferred method when a representative sample is needed. This method produces unbiased estimates of the population, as each unit has an equal probability of being chosen.

Final Report: Results

Survey results from responding covered entities regarding the audit report issued to them:

• **80%**
  The report was clear and easy to read

• **79%**
  The report provided an actionable basis for bringing the entity into HIPAA compliance

• **71%**
  The report adequately identified gaps between HIPAA requirements and entity operations
Who will be audited & selection
What will be audited
Approach
Timeline
Outreach
Electronic management system

PHASE 2  2014 -- 2015

Who Can Be Audited?

- Any Covered Entity
  - Health plans of all types
  - Health care clearinghouses
  - Individual and organizational providers

- Any Business Associate
  - Selection through covered entities
Phase 2 Covered Entity Pool

- Have selected a pool of covered entities eligible for audit
- Used resources developed through Booz Allen Hamilton contract
  - Health care providers selected through NPI database
  - Clearinghouses & Health Plans from external databases (e.g., AHIP)
- Random selection used when possible w/in types
- Wide range (e.g., group health plans, physicians and group practices, behavioral health, dental, hospitals, laboratories)

Pre-audit Survey

- Available entity databases lack data for entity stratification
- Survey currently going through the Paperwork Reduction Act clearance process
- Questions address size measures, location, services, best contacts
- OCR will conduct address verification with entities this spring
- Entities will receive link to on-line screening “pre-survey” this summer
- Expect to contact 550-800 entities
- OCR will use results of survey to select a projected 350 covered entities to audit
Audit Phase 2 Approach

- Primarily internally staffed
- Selected entities will receive notification and data requests in fall 2014
- Entities will be asked to identify their business associates and provide their current contact information
- Will select business associate audit subjects for 2015 first wave from among the BAs identified by covered entities
- Desk audits of selected provisions
- Comprehensive on-site audits as resources allow

Phase 2 Audit Distribution Projections

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>Privacy</th>
<th>Breach</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered Entities</td>
<td>100</td>
<td>100</td>
<td>150</td>
</tr>
<tr>
<td>• Health Plans</td>
<td>33</td>
<td>31</td>
<td>45</td>
</tr>
<tr>
<td>• Providers</td>
<td>67</td>
<td>65</td>
<td>100</td>
</tr>
<tr>
<td>• Clearinghouses</td>
<td>-</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Business Associates</td>
<td>0</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td>• IT Related</td>
<td>-</td>
<td>-</td>
<td>35</td>
</tr>
<tr>
<td>• Non-IT Related (eg, TPAs, claims)</td>
<td>-</td>
<td>-</td>
<td>15</td>
</tr>
<tr>
<td>Total Audits by Protocol</td>
<td>100</td>
<td>100</td>
<td>200</td>
</tr>
</tbody>
</table>
Phase 2 Desk Audits

- Pre-audit survey links to pool
  - Summer 2014

- Notification and data request to selected entities
  - Fall 2014

- Desk review and draft findings

- Entity provides management review

- Final report

Phase 2 Timing

<table>
<thead>
<tr>
<th>Period</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spring 2014</td>
<td>CE address verification</td>
</tr>
<tr>
<td>Summer 2014</td>
<td>Pre-audit surveys link sent to covered entity pool</td>
</tr>
<tr>
<td>Fall 2014</td>
<td>Notification and data request letters to selected entities</td>
</tr>
<tr>
<td>Two weeks</td>
<td>Period for entity response</td>
</tr>
<tr>
<td>October 2014 -- June 2015</td>
<td>CE Audit Reviews</td>
</tr>
<tr>
<td>2015</td>
<td>Business Associates</td>
</tr>
</tbody>
</table>
### Desk Audit Expectations

Data request will specify content & file organization, file names, and any other document submission requirements

Only requested data submitted on time will be assessed.

All documentation must be current as of the date of the request.

Auditors will not have opportunity to contact the entity for clarifications or to ask for additional information, so it is critical that the documents accurately reflect the program.

Submitting extraneous information may increase difficulty for auditor to find and assess the required items.

Failure to submit response to requests may lead to referral for regional compliance review

### Electronic Management System

- All communication electronic—entities will receive and respond to pre-audit survey, notification and document requests through email, or other electronic media (eg, CD)

Audit management system for
- Document retention
- Auditor assignments
- Work papers
- Audit manager review
- Referral for regional compliance review
Phase 2 Protocol Criteria

- Auditors will assess entity efforts through an updated protocol; new criteria reflect omnibus rule changes and more specific test procedures
- Uses sampling methodology in a number of provisions to assess compliance efforts
- Desk audits will target particular provisions that were the source of a high number of compliance failures in the pilot audits
- Updated protocol will be available on web site so that entities can use it for internal compliance assessments

Phase 2 Audit Focus

**2014 – Covered Entities**
- Security—Risk analysis and risk management
- Breach—Content and timeliness of notifications
- Privacy—Notice and Access

**2015**

*Round 1 Business Associates*
- Security—Risk analysis and risk management
- Breach—Breach reporting to CE

*Round 2 Covered Entities (Projected)*
- Security—Device and media controls, transmission security
- Privacy—Safeguards, training to policies and procedures

**2016 (Projected)**
- Security: Encryption and decryption, facility access control (physical); other areas of high risk as identified by 2014 audits, breach reports and complaints
EHR & HIPAA on Medscape

• New! 6th module EHRs and HIPAA: Steps for Maintaining the Privacy and Security of Patient Information."

• For physicians, nurses, and other healthcare professionals; free Continuing Medical Education (CME) and Continuing Education (CE) credits. Steps to safeguard patient data on electronic health records (EHRs), to plan appropriate communication for patients about how their data will be stored and used on EHRs, and to evaluate Meaningful Use criteria related to data security and privacy required as part of the EHR Incentive Program.


Medscape Education Tools

• Patient Privacy: A Guide for Providers

• HIPAA and You: Building a Culture of Compliance

• Examining Compliance with the HIPAA Privacy Rule

• These Medscape modules offer free Continuing Medical Education (CME) credits for physicians and Continuing Education (CE) credits for health care professionals.
Security Rule Compliance Aides

- **New!** Risk Analysis tool for small providers from ONC, find at http://healthit.gov
- **HHS Mobile Device Security Resource Kit**
  - [http://healthit.gov/mobiledevices](http://healthit.gov/mobiledevices)
- **Vast Array of Guidance Material**

More Information

**HIPAA Audit Webpage**


Wide range of other information about health information privacy including educational resources, FAQ’s, rule text and guidance for the Privacy, Security, and Breach Notification Rules