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>
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)
Performance Audit Objective

To analyze the key processes, controls, and policies of the auditee relative to selected requirements of the Rules as specified in an OCR audit protocol and provide findings or observations.

The audit objective did not include a determination of the effectiveness of implementation of the selected requirements in OCR’s audit protocol.
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)
OCR identified a pool of covered entities

- Type of entity
- Geographic location
- Public versus Private
- Specific criteria includes but is not limited to:
  - Entity’s size, e.g., level of revenues/assets, number of patients or employees, use of HIT
  - Affiliation with other health care organizations

IAPP - March 7, 2013
Breakdown of 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

IAPP - March 7, 2013
## Auditees by Type & Size

<table>
<thead>
<tr>
<th>Health 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>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><strong>Total</strong></td>
<td><strong>26</strong></td>
<td><strong>31</strong></td>
<td><strong>22</strong></td>
<td><strong>36</strong></td>
<td><strong>115</strong></td>
</tr>
</tbody>
</table>

IAPP - March 7, 2013
Audit Process
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

IAPP - March 7, 2013
Planning the Audit

1. Complete Covered Entity selection process to:
   - Determine auditee universe;
   - Determine independence from entity;
   - Determine entity size and type; and
   - Select the entity.
2. Send notification letter to the selected Covered Entity including:
   - Information Request List; and
   - Entity Survey.
3. Make Initial contact to:
   - Confirm Notification Letter receipt;
   - Respond to any questions/concerns; and
   - Confirm due date for documentation requests.
Preparation Work

1. Conduct kick-off call to:
   - Confirm Covered Entity type (provider, clearinghouse, fully insured group health plan, etc.), applicable scope, audit location(s); and
   - Discuss on-site visit and logistics.

2. Perform analysis of documentation provided by the Covered Entity to determine:
   - What documents have been received; and
   - What documents are missing?

3. Begin audit testing procedures surrounding the review of documentation.

4. Send field work start date reminder email.
Field Work

1. Conduct an entrance conference with the Covered Entity to discuss:
   - Performance audit concept, scope, objective, and approach; and
   - Set expectations with the auditee.

2. Execute and document all applicable audit procedures (see *Audit Protocol Walkthrough*):
   - Complete onsite testing;
   - Conduct interviews;
   - Review documentation; and
   - Observe appropriate facilities/workstations.

3. Conduct an exit conference with the Covered Entity to discuss:
   - Preliminary identified issues; and
   - Discuss next steps for the audit process.
Post Field Work

1. Document results of the audit.
2. Finalize draft identified findings.
4. Submit draft audit report and supporting evidence for Quality Assurance (QA) Review.
5. Provide draft findings to Covered Entity for management response.
6. Incorporate findings with management responses into draft report and Clarify management responses with Covered Entity.
7. Submit draft audit report and results for secondary QA Review.
8. Provide OCR with draft audit report for comments.
10. Issue the final audit report.
Audit Process Walkthrough
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
Audit Protocol Components

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.
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.
Audit Testing Procedure - Review

• The audit team would execute this audit step through review of documentation:
  - For providers only: obtain and review all patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any.
Workpaper - Authorizations

• Results of Audit Testing Procedure
  - Documentation of the procedures performed and audit evidence obtained

• Summary of Results
  - Documentation of whether the Covered Entity addressed the requirements outlined within the criteria.
  - Documentation of a reference to a finding.
Appendix A - Tested Privacy & Breach Notification Protocol
# Privacy Audit Protocol

<table>
<thead>
<tr>
<th>Section</th>
<th>Key Activity</th>
<th>W/P Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AA. Notice of Privacy Practices - §164.520</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.520</td>
<td>Notice of Privacy Practices</td>
<td>EF-320.AA</td>
</tr>
<tr>
<td>§164.520</td>
<td>Provision of Notice - Health Plans</td>
<td>EF-321.AA</td>
</tr>
<tr>
<td>§164.520</td>
<td>Provision of Notice - Certain Covered Health Care Providers</td>
<td>EF-322.AA</td>
</tr>
<tr>
<td>§164.520</td>
<td>Provision of Notice - Electronic Notice</td>
<td>EF-323.AA</td>
</tr>
<tr>
<td>§164.520</td>
<td>Joint Notice by Separate Covered Entities</td>
<td>EF-324.AA</td>
</tr>
<tr>
<td><strong>BB. Rights to Request Privacy Protection for PHI - §164.522</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.522</td>
<td>Confidential Communication Requirements</td>
<td>EF-325.BB</td>
</tr>
<tr>
<td><strong>CC. Access of Individuals to PHI - §164.524</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.524</td>
<td>Right to Access</td>
<td>EF-330.CC</td>
</tr>
<tr>
<td>§164.524</td>
<td>Review of Denial of Access</td>
<td>EF-331.CC</td>
</tr>
<tr>
<td><strong>DD. Administrative Requirements - §164.530</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.530</td>
<td>Privacy Training</td>
<td>EF-335.DD</td>
</tr>
<tr>
<td>§164.530</td>
<td>Complaints to the Covered Entity</td>
<td>EF-336.DD</td>
</tr>
<tr>
<td>§164.530</td>
<td>Sanctions of Workforce Regarding failure to Comply with the Privacy Policies and Procedures</td>
<td>EF-337.DD</td>
</tr>
<tr>
<td>§164.530</td>
<td>Policies and Procedures</td>
<td>EF-338.DD</td>
</tr>
</tbody>
</table>
# Privacy Audit Protocol - U&D

<table>
<thead>
<tr>
<th>Section</th>
<th>Key Activity</th>
<th>W/P Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF. Uses and Disclosures § 164.502, 504, 508, 510, 512, and 514</td>
<td>§164.502 Deceased Individuals</td>
<td>EF-345.FF</td>
</tr>
<tr>
<td></td>
<td>§164.502 Personal Representatives</td>
<td>EF-346.FF</td>
</tr>
<tr>
<td></td>
<td>§164.504 Business Associate Contracts</td>
<td>EF-347.FF</td>
</tr>
<tr>
<td></td>
<td>§164.504 Requirements for Group Health Plans</td>
<td>EF-348.FF</td>
</tr>
<tr>
<td></td>
<td>§164.506 Permitted Uses and Disclosures</td>
<td>EF-349.FF</td>
</tr>
<tr>
<td></td>
<td>§164.508 Obtaining Authorization as Required for Internal Use and Disclosure of Protected Health Information</td>
<td>EF-350.FF</td>
</tr>
<tr>
<td></td>
<td>§164.508 Authorization for Uses and Disclosures is Required</td>
<td>EF-351.FF</td>
</tr>
<tr>
<td></td>
<td>§164.510 Limited Uses and Disclosures when the Individual is Not Present</td>
<td>EF-352.FF</td>
</tr>
<tr>
<td></td>
<td>§164.512 Disclosures for Judicial and Administrative Proceedings</td>
<td>EF-353.FF</td>
</tr>
<tr>
<td></td>
<td>§164.512 Uses and Disclosures for Research Purposes</td>
<td>EF-354.FF</td>
</tr>
<tr>
<td></td>
<td>§164.512 Re-Identification</td>
<td>EF-355.FF</td>
</tr>
<tr>
<td></td>
<td>§164.514 Minimum Necessary Uses of PHI</td>
<td>EF-356.FF</td>
</tr>
<tr>
<td></td>
<td>§164.514 Minimum Necessary Disclosures of PHI</td>
<td>EF-357.FF</td>
</tr>
<tr>
<td></td>
<td>§164.514 Uses and Disclosures for Fundraising</td>
<td>EF-358.FF</td>
</tr>
<tr>
<td></td>
<td>§164.514 Uses and Disclosures for Underwriting and Related Purposes</td>
<td>EF-359.FF</td>
</tr>
<tr>
<td></td>
<td>§164.514 Verification of the Identity of Those Requesting PHI</td>
<td>EF-360.FF</td>
</tr>
</tbody>
</table>
## Breach Notification Rule

<table>
<thead>
<tr>
<th>Section</th>
<th>Key Activity</th>
<th>W/P Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>EE. Breach Notification- §164.404 and 414</td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.404</td>
<td>Notification to Individuals</td>
<td>EF-340.EE</td>
</tr>
<tr>
<td>§164.404</td>
<td>Timeliness of Notification</td>
<td>EF-341.EE</td>
</tr>
<tr>
<td>§164.404</td>
<td>Methods of Individuals Notification</td>
<td>EF-342.EE</td>
</tr>
<tr>
<td>§164.414</td>
<td>Burden of Proof</td>
<td>EF-343.EE</td>
</tr>
</tbody>
</table>
Appendix B - Tested Security Protocol
## Security Audit Protocol

<table>
<thead>
<tr>
<th>Section</th>
<th>Key Activity</th>
<th>W/P Ref.</th>
<th>Implementation Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A. Administrative Safeguards - §164.308</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.308(a)(1)</td>
<td>Conduct Risk Assessment</td>
<td>EF-301.A</td>
<td>Required</td>
</tr>
<tr>
<td>§164.308(a)(7)</td>
<td>Develop Contingency Planning Policy</td>
<td>EF-305.A</td>
<td>Required</td>
</tr>
<tr>
<td><strong>A. Physical Safeguards - §164.310</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.310(c)</td>
<td>Identify All Methods of Physical Access to Workstations</td>
<td>EF-310.B</td>
<td>Required</td>
</tr>
<tr>
<td>§164.310(c)</td>
<td>Implement Methods for Final Disposal of ePHI</td>
<td>EF-311.B</td>
<td>Required</td>
</tr>
<tr>
<td>§164.310(d)(1)</td>
<td>Maintain Accountability for Hardware and Electronic Media</td>
<td>EF-312.B</td>
<td>Addressable</td>
</tr>
<tr>
<td>§164.310(d)(1)</td>
<td>Develop Data Backup and Storage Procedures</td>
<td>EF-313.B</td>
<td>Addressable</td>
</tr>
<tr>
<td><strong>C. Technical Safeguards - §164.312</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.312(a)(1)</td>
<td>Encryption and Decryption</td>
<td>EF-315.C</td>
<td>Addressable</td>
</tr>
<tr>
<td>§164.312(b)</td>
<td>Determine the Activities that Will be Tracked or Audited</td>
<td>EF-316.C</td>
<td>Required</td>
</tr>
<tr>
<td>§164.312(b)</td>
<td>Implement the Audit/System Activity Review Process</td>
<td>EF-317.C</td>
<td>Required</td>
</tr>
<tr>
<td>§164.312(c)(1)</td>
<td>Identify All Users Who Have Been Authorized to Access ePHI</td>
<td>EF-318.C</td>
<td>N/A</td>
</tr>
<tr>
<td>§164.312(c)(1)</td>
<td>Implement a Mechanism to Authenticate ePHI</td>
<td>EF-319.C</td>
<td>Addressable</td>
</tr>
</tbody>
</table>
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.
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
Proportional by Entity Type

Audit Findings and Observations by Type of Covered Entity
Proportional Findings by Rule

Audit Findings and Observations by Rule
Element Exposure by Entity Type

Audit Findings and Observations Distribution
Privacy Findings & Observations

PERCENTAGE OF FINDINGS AND OBSERVATIONS BY AREA OF FOCUS
Privacy Results by Entity Type

Findings and Observations by Area and Type of Entity
Privacy Results by Entity Size

**Findings and Observations by Level**

![Graph showing findings and observations by level for various areas of focus.]
Privacy Administrative Elements

Administrative Requirements Findings and Observations

IAPP - March 7, 2013
Privacy -- Uses and Disclosures

Uses and Disclosures of PHI Findings and Observations
Individual HIPAA Privacy Area of Focus - Audit Findings and Observations

Notice of Privacy Practices for PHI Findings and Observations

Notice of Privacy Practices for PHI Unaudited Observations*

*The graph on the bottom includes an analysis of observations from additional areas of the Notice of Privacy Practice content requirements that were not included in the
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: Almost every entity without a finding or observation met by fully implementing the addressable specification.
Security Elements

Percentage of Audit Findings and Observations by Area of Focus
Security by Entity Type

Total Audit Findings and Observations by Area of Focus and Entity Type
Security Results by Entity Size

Total Security Audit Findings and Observations by Area of Focus and Level of Entity
Breach Notification by Entity Type

Audit Findings and Observations by Requirement and Type of Entity
Breach Notification by Entity Size

Audit Findings and Observations by Requirement and Level 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>
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?
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/

Linda Sanches  linda.sanches@hhs.gov
Verne Rinker  verne.rinker@hhs.gov