OCR Phase II Audits: What is Happening?

Presented by:
Marti Arvin
Vice President of Audit Strategy, CynergisTek

Today’s Presenter

- Vice President of Audit Strategies, CynergisTek, Inc.
- Subject matter expert on healthcare compliance programs with a focus on the HIPAA Privacy, Security and Breach Notification Rules
- Experienced in developing, implementing and evaluating compliance programs for large and small organizations
- Holds the CHC-F, CCEP-F, CHPC and CHRC certifications
Agenda

<table>
<thead>
<tr>
<th>Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCR HIPAA Audit Program</td>
</tr>
<tr>
<td>OCR HIPAA Desk Audits</td>
</tr>
<tr>
<td>OCR HIPAA Compliance Performance Audits</td>
</tr>
<tr>
<td>Creating an OCR Audit Toolkit</td>
</tr>
<tr>
<td>Questions</td>
</tr>
</tbody>
</table>
HIPAA/HITECH Audits

HITECH Act – Sec. 13411
- Periodic audits to ensure covered entities and business associates comply with requirements of HIPAA and HITECH
- Examine mechanisms for compliance
- Identify best practices
- Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
- Renew attention of covered entities to health information privacy and security compliance activities

Concerns About HIPAA Compliance

- 281,000 breaches reported to HHS since 2010
- 1,724 large breaches (>500) have disclosed PHI as of 10/26/16 (114.3 million records)
- 60% incidents due to loss/theft unencrypted laptops, media and portable/mobile devices
- Hacking/IT network breaches account for 70% of records disclosed
- Business associates account for 1 in 4 large breaches
- 140,000 individual complaints alleging HIPAA violations
Enforcement Sets Audit Priorities

- $23.5 million paid to OCR for HIPAA violations in 2016 as of 11/28/16
- Key issues highlighted in resolution agreements:
  - Business Associate Agreements
  - Risk Analysis
  - Failure to manage identified risk, e.g. encrypt
  - No patching of software
  - Insider threat
  - Improper disposal
  - Insufficient data backup and contingency planning

Today: OCR’s Permanent Audit Program

- 14,000 covered entities received request for contact & questionnaire
- 167 covered entities selected for desk audit
  - CEs queried on OCR compliance with Security Rule or Privacy/Breach Rules
  - All CEs provide business associate names and contact information
    http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html
- Fall 2016: 40-50 business associates selected for desk audit
- Early 2017: Small number of onsite, comprehensive audits
- 2017: Will OCR use HIPAA $$ for larger audit program?
Audit Selection Criteria

- Size and Use of HIT
- Geographic Location
- Criteria Used in Pool of CEs
- Affiliations with Other CEs
- Type of Entity

OCR Desk Audit Program
HIPAA Desk Audits

- Data request will specify content and other electronic document submission requirements
- 10 business days to respond
- Only the documentation submitted on time is reviewed
- All documentation must be current as of the date of the request

- Auditors will not be able to contact the entity for clarifications or ask for additional information
  - Critical that documentation accurately reflects the program
- Submission of extraneous information increases difficulty for auditor in finding/assessing required items
- Failure to submit responses leads to compliance review

Steps to the Desk Audit

Pre-Audit Survey | Notification and data request to selected entities | Desk review and draft findings to entity | Entity provides management review | Final Report
Scope of OCR Desk Audits

2016 Desk Audits of Covered Entities
- **Security** - Risk Analysis and risk management
- **Breach** - Content and timeliness of breach notifications
- **Privacy** - Notice of Privacy Practices and Access

2016 Desk Audits of Business Associates
- **Security** - Risk Analysis and risk management
- **Breach** - Breach reporting to covered entities

2017 On-site Comprehensive Audits
- **Covered entities**
- **Business associates**

Desk Audit Protocol Risk Management

<table>
<thead>
<tr>
<th>Documentation Requested</th>
<th>What Should be Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload documentation demonstrating the security measures implemented to reduce the risks as a result of the current risk analysis or assessment</td>
<td>Provide documentation that the organization has implemented or has plans to implement administrative, physical or technical controls to reduce risks and vulnerabilities identified in the current risk analysis.</td>
</tr>
<tr>
<td>Upload documentation demonstrating that policies and procedures related to implementing risk management processes have been in place and in force for the prior 6 years.</td>
<td>Provide documentation of current and prior versions of risk management policies and procedures from 2010 to 2016. These policies and procedures should identify how risk is managed, what the organization considers an acceptable level of risk in its management program, the frequency of reviewing ongoing risks, and identify the workforce members who are assigned a role in the risk management process.</td>
</tr>
<tr>
<td>Upload documentation demonstrating the efforts used to manage risks from the previous calendar year.</td>
<td>Provide documentation for the 2015 calendar year of the actions the organization took, or had plans to take, to implement administrative, physical or technical controls to reduce risks and vulnerabilities identified in its risk analysis.</td>
</tr>
</tbody>
</table>
## Desk Audit Protocol Breach Management

<table>
<thead>
<tr>
<th>Documentation Requested</th>
<th>What Should be Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using sampling methodologies, upload documentation of 5 breach incidents for the previous calendar year affecting &lt;500 individuals, documenting the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification.</td>
<td>Prepare summary reports of 5 small breaches that occurred in 2015 with information of when the breach was discovered, the date individuals were notified, and the reason, if any, for a delay in notification. Organizations can submit copies of internal incident response reports if they contain the documentation required.</td>
</tr>
<tr>
<td>If the covered entity used a standard template or form letter to notify individuals of a breach, upload the document.</td>
<td>Provide a sample copy of breach notification letter(s).</td>
</tr>
<tr>
<td>Using sampling methodologies, upload documentation of 5 breach incidents for the previous calendar year affecting &gt;500 individuals.</td>
<td>Prepare summary reports of 5 large breaches that occurred in 2015 with information of when the breach was discovered, the date individuals were notified, and the reason, if any, for a delay in notification. Organizations can submit copies of internal incident response reports if they contain the documentation required.</td>
</tr>
</tbody>
</table>

## Desk Audit Protocol Patient Access

<table>
<thead>
<tr>
<th>Documentation Requested</th>
<th>What Should be Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year.</td>
<td>Prepare summary reports of the first 5 requests received in 2015 in which the patient or their representative was provided access to, or copies of, the individual’s PHI. Provide copies of written documents of the request and when &amp; how the request for access or copies of the PHI was sent.</td>
</tr>
<tr>
<td>Upload all documentation related to the last 5 access requests which were granted, and evidence of fulfillment the previous calendar year.</td>
<td>Prepare summary reports of the last 5 requests received in 2015 in which the patient or their representative was provided access to, or copies of, the individual’s PHI. Provide copies of written documents of the request and when &amp; how the request for access or copies of the PHI was sent.</td>
</tr>
<tr>
<td>Upload policies and procedures for individuals to request and provision of (access) to their health information.</td>
<td>Provide documentation of current policies and procedures for standards and implementation specifications for 45 CFR 164.524 (a)-(d).</td>
</tr>
</tbody>
</table>
On-Site Comprehensive Audits

On-Site Audits = Performance Audits

• Conducted in accordance with Generally Accepted Government Audit Standards (GAGAS)
• Provides findings, observations, or conclusions from evaluation of evidence against established criteria
• Objective assessment of variety of attributes:
  – Program effectiveness, economy, and efficiency
  – Internal controls
  – Compliance
On-Site Audits Timeline

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Elapsed Time</th>
<th>Notification</th>
<th>Receiving and reviewing documentation and planning the audit fieldwork</th>
<th>On-site fieldwork</th>
<th>Draft audit report</th>
<th>Covered entities review and comment on draft audit reports</th>
<th>Final audit report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1</td>
<td>Day 10</td>
<td>1 Day</td>
<td>Day 10</td>
<td>3 – 10 Days</td>
<td>20 – 30 Days</td>
<td>10 Days</td>
<td>30 Days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum of 10 Days</td>
<td>10 Days</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Planning the On-Site Audit

- Send notification letter to the covered entity
  - Information request list
  - Entity survey
- Make initial telephone contact with covered entity
  - Confirm notification letter receipt
  - Respond to questions and concerns
  - Confirm due date for documentation
**Documentation Request**

<table>
<thead>
<tr>
<th>Checklist Category</th>
<th>Document Name/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information</td>
<td>Size of CE, number of employees, members or patients, facilities EMR facility (Y/N)</td>
</tr>
<tr>
<td>HIPAA Security</td>
<td>ID any application industry guidance (e.g. studies, practices, regulations, etc.) or other reference material used to develop any of the policies and procedures requested below (no need to provide this document, just identify) Security office contact info (name, email, phone, address &amp; admin contact info)</td>
</tr>
<tr>
<td>Administrative Safeguards</td>
<td>Entity-level risk assessment</td>
</tr>
<tr>
<td></td>
<td>Organizational chart</td>
</tr>
<tr>
<td></td>
<td>Information security policies, specially those documenting security management practices &amp; processes, such as access control, data protection, and more</td>
</tr>
</tbody>
</table>

**Pre-Audit Preparation**

- Conduct kick-off call
  - Confirm covered entity type (e.g. provider, health plan), applicable scope, audit location(s)
  - Discuss on-site visit and logistics
- Perform analysis of documentation provided by CE
  - What documents have been received and which are missing
  - Review documentation for compliance with appropriate regulatory standard or specification
On-Site Field Work

- Conduct entrance conference
  - Discuss performance audit scope, objective and approach
  - Set expectations
- Execute and document applicable audit procedures
  - Complete on-site testing
  - Conduct interviews
  - Review documentation
  - Observe appropriate facilities and workstations
- Conduct exit conference
  - Preliminary identification of compliance issues

Post On-Site Field Work

- Document results of the audit
- Finalize draft identified findings
- Issue draft performance report to CE for comment and correction
- Issue final performance audit report that includes CE comments and response
**OCR On-Site Audit Scope**

**Security**
- Device and media controls
- Transmission security
- Encryption of data at rest
- Facility access controls

**Privacy**
- Administrative and physical safeguards
- Workforce training to HIPAA policies & procedures
- Individual access to PHI in electronic format

**Other Areas**
- High risk areas identified through:
  - 2016 desk audits
  - Breach reports submitted to OCR
  - Consumer complaints

**Sample Audit Protocol - Provider**

<table>
<thead>
<tr>
<th>Breach Notification</th>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assessment for breach</td>
<td>• Notice of Privacy Practices</td>
<td>• Administrative Safeguards</td>
</tr>
<tr>
<td>• Notification to individuals</td>
<td>• Request Restrictions</td>
<td>• Physical Safeguards</td>
</tr>
<tr>
<td>• Notification to Secretary</td>
<td>• Right to Access</td>
<td>• Technical Safeguards</td>
</tr>
<tr>
<td>• Notification to media</td>
<td>• Administrative Requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Amendment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Uses &amp; Disclosures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accounting of Disclosures</td>
<td></td>
</tr>
</tbody>
</table>
HIPAA Security Risk Assessment

- Required element for Security Rule and Meaningful Use
- An assessment of threats and vulnerabilities to information systems that handle e-PHI
- This provides the starting point for determining what is ‘appropriate’ and ‘reasonable’
- Organizations determine their own technology and administrative choices to mitigate their risks
- The risk analysis process should be ongoing and repeated as needed when the organization experiences changes in technology or operating environment

Performing a Risk Analysis

- **Gather Information**
  - Prepare inventory lists of information assets-data, hardware and software.
  - Determine potential threats to information assets.
  - Identify organizational and information system vulnerabilities.
  - Document existing security controls and processes.

- **Analyze Information**
  - Evaluate and measure risks associated with information assets.
  - Rank information assets based on asset criticality and business value.
  - Develop and analyze multiple potential threat scenarios.

- **Develop Remedial Plans**
  - Prioritize potential threats based on importance and criticality.
  - Develop remedial plans to combat potential threat scenarios.
  - Repeat risk analysis to evaluate success of remediation and when there are changes in technology or operating environment.
Building an Audit Toolkit

Components of an Audit Toolkit

- Pre-Audit Survey Questionnaire

- Requirements for listing business associates

- OCR's 2016 Audit Protocol
### Notification to Individuals

#### Key Activity

<table>
<thead>
<tr>
<th>Uses and disclosures required by law</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.512(a)(1) - A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies and is limited to the relevant requirements of such law.</td>
</tr>
<tr>
<td>§164.512(a)(2) - A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit Inquiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the covered entity use and disclose PHI pursuant to requirements of other law? If so, are such uses and disclosures made consistent with the requirements of this performance criterion as well as the applicable requirements related to victims of abuse, neglect or domestic violence, pursuant to judicial and administrative proceedings and law enforcement purposes of this section? Obtain and review policies and procedures for uses and disclosures required by law.</td>
</tr>
</tbody>
</table>

#### Key Activity

<table>
<thead>
<tr>
<th>Notice to Individuals of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.404(a)(1) - Notice to Individuals. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit Inquiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the covered entity have policies and procedures for notifying individuals of a breach of their protected health information.</td>
</tr>
</tbody>
</table>

Obtain and review a list of breaches, if any, in the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the affected individuals. Determine whether notifications were provided to individuals consistent with the requirements in §164.404(a)(1).
Questions

Questions?

Marti Arvin
marti.arvin@cynergistek.com
512.405.8550 x7051