Update on Audits of Entity Compliance with the HIPAA Rules

Linda Sanches
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

September, 2017
Purpose

Phase 2 Audit Program
Status, Process, Protocol

Preliminary Findings

Guidance
Support Improved Compliance

- Identify best practices; uncover risks & vulnerabilities; detect areas for technical assistance; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open up compliance review (for example, if significant concerns are raised during an audit or an entity fails to respond)
- Learn from this phase in structuring permanent audit program
- Develop tools and guidance for industry self-evaluation and breach prevention
• Desk audits of covered entities complete
• Desk audits of business associates underway
• Business associate selection pool largely drawn from over 20,000 entities identified by audited CEs
• On-site audits of both CEs and BAs after completion of the desk audit process, to evaluate against a comprehensive selection of controls in protocols
• Desk audit subject may be subject to on-site audit
CE Audits (166)
• Privacy and Breach (103)
• Security (63)

BA Audits (41)
• Breach and Security
2016 Audited Covered Entities

- Provider: 90%
- Health Plan: 8.7%
- Health Care Clearinghouse: 1%
After review of submitted documentation
• draft findings shared with the entity,
• Entity may respond in writing

Final audit reports will
• describe how the audit was conducted,
• present any findings, and
• contain any written entity responses to the draft

Under OCR’s separate, broad authority to open compliance reviews, OCR could decide to open a separate compliance review in a circumstance where significant threats to the privacy and security of PHI are revealed through the audit
Failure to Respond

- Email notice to verify contact information
- Pre-audit screening questionnaire
- Document request notification
- Entities who fail to respond, remain in the audit pool & may be subject to compliance review
| Privacy Rule Controls | Notice of Privacy Practices & Content Requirements  
[S164.520(a)(1) & (b)(1)] |
|-----------------------|-----------------------------------------------------------------------------|
|                       | Provision of Notice – Electronic Notice  
[S164.520(c)(3)] |
|                       | Right to Access  
[S164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)] |
| Breach Notification | Timeliness of Notification  
[S164.404(b)] |
| Rule Controls         | Content of Notification  
[S164.404(c)(1)] |
[S164.308(a)(1)(ii)(A)] |
| Controls             | Security Management Process -- Risk Management  
[S164.308(a)(1)(ii)(B)] |
<table>
<thead>
<tr>
<th>Breach Notification Rule Controls</th>
<th>Notification by a Business Associate [§164.410, with reference to Content of Notification §164.404(c)(1)]</th>
</tr>
</thead>
</table>
• Notice of Privacy Practices
  ✓ Copy of all notices including URL of notice posted on the entity website, electronic notice policy and procedures

• Right to Access
  ✓ Access requests, extensions to access requests, access requests templates/forms, NOPP, access policies and procedures

• Timeliness of Notification
  ✓ Documentation for five small and large breaches incidents

• Content of Notification
  ✓ Five large breach incidents, breach template/form, copy of a single written notice
• Risk Analysis

✓ Current and prior risk analysis and results
✓ Policies and procedures of the risk analysis process
✓ Policies and procedures related to the implementation of risk analysis 6 years prior to the date of audit notification
✓ Documentation from the previous year demonstrating implementation of risk analysis process, how it is available to persons responsible for process and evidence the documentation is periodically reviewed and updated, as needed
• **Risk Management**
  - Documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment
  - Documentation demonstrating the efforts used to manage risks from the previous calendar year
  - Policies and procedures of the risk management process
  - Policies and procedures related to the implementation of risk management for the prior 6 years of the date of audit notification
  - Documentation demonstrating the current and ongoing risks reviewed and updated
  - Documentation from the previous year demonstrating implementation of the risk management process, how it is available to persons responsible for the risk management process and evidence the documentation is periodically reviewed and updated, as needed
<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.</td>
</tr>
<tr>
<td>2</td>
<td>The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.</td>
</tr>
<tr>
<td>3</td>
<td>Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.</td>
</tr>
<tr>
<td>4</td>
<td>Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.</td>
</tr>
<tr>
<td>5</td>
<td>The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.</td>
</tr>
</tbody>
</table>
Anatomy of an Audit Report

- Introduction
- Audit Objective
- Background
- Scope and Methodology
- Results of Review
- Auditor Ratings Legend
- Summary of Auditor Ratings
- Auditor Analysis & Findings
  - Element #
  - Auditor’s Analysis
  - Effect
  - Finding
  - Ratings
  - Entity Response
### Rating Poles

<table>
<thead>
<tr>
<th></th>
<th>5 Rating</th>
<th>1 Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach T 103</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeliness of Notification</td>
<td>15</td>
<td>67</td>
</tr>
<tr>
<td>Content of Notification</td>
<td>9</td>
<td>14</td>
</tr>
<tr>
<td>Privacy T 103</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>Notice Content</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>eNotice</td>
<td>15</td>
<td>59</td>
</tr>
<tr>
<td>Security T 63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>Risk Management</td>
<td>17</td>
<td>1</td>
</tr>
</tbody>
</table>
BNR 12 -- Timeliness of Notification

Ratings
- 1
- 2
- 3
- 4
- 5
- N/A
BNR 13 -- Content of Notification

Ratings
- 1
- 2
- 3
- 4
- 5
- N/A
P55 -- Notice of Privacy Practices -- Content

Ratings

1
2
3
4
5

2% 15% 11% 39% 33%
P58 - Provision of Notice

Ratings

- 1: 57%
- 2: 15%
- 3: 6%
- 4: 15%
- 5: 3%
- N/A: 15%
P65 -- Right to Access

Ratings

- 1
- 2
- 3
- 4
- 5
S 2  Security Risk Analysis Ratings
63 Covered Entities
S 3 Risk Management Ratings

17
1
3
13
29

Ratings
1
2
3
4
5
Selected protocol elements with associated document submission requests and related Q&As

Slides from audited covered entity webinar held July 13, 2016

Comprehensive question and answer listing

OCR Audit Website:
http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html
Visit the Website

http://www.hhs.gov/hipaa

Join us on @hhsocr
For additional information contact:

Zinethia L. Clemmons
HIPAA Compliance Audit Program Director
zinethia.clemmons@hhs.gov