How to Prepare for an OCR Audit

April 2015
HCCA Compliance Institute

Presented by
Elizabeth Callahan-Morris, Hall Render
Margaret Marchak, Hartford HealthCare

Headlines

• 2 recent cybersecurity breaches affecting 91 million plan members in total
• Proposed national data breach notification standard
• Executive orders on cybersecurity
• Medical devices
• FTC enforcement actions
• Health care going global
• Cost of data breaches
HIPAA Enforcement Actions

- As of early 2015, over $25M in OCR settlements and CMPs
  - 23 enforcement actions
  - $1M average settlement
  - OCR warns this is just the beginning
  - State enforcement
Recent OCR HIPAA Settlements

- AK community mental health agency $150,000 for malware exposure (Dec 2014)
- IN health system - $800,000 for medical records dumping (July 2014)
- NY hospital - $3.3M for PHI accessible over internet (May 2014)
- NY university - $1.5M for PHI accessible over internet (May 2014)
- MO PT Center - $1.7M for stolen laptop (April 2014)
- AR health Plan - $250,000 for stolen laptop (April 2014)
- WA county govt - $215,000 for ePHI on public server (March 2014)

Other Enforcement Actions & Regulatory Activity

- DOJ
- FTC
- FCC
- State Attorneys General
- State licensing boards
- Joint Commission
- Meaningful use
- Individual and class-action lawsuits
- False Claims Act??
OCR Audit Program Phase 1

- HITECH requires HHS (OCR) to perform periodic audits of CE and BA compliance with HIPAA Privacy, Security, and Breach Notification Rules
- OCR established a pilot audit program to assess the controls and processes CEs implemented to comply
- In this program, OCR developed a protocol used to gauge efforts of 115 CEs in 2011-2013
- External auditors utilized
- Findings published

Scenario

- CE received audit notice from OCR and KPMG
- Request for documents and information
- Date for KPMG auditors to meet at the CE on-site
- 20 initial audits
- Field work 1/12 to 3/12
OCR Audit Program Phase 1

• Most common Privacy Rule deficiencies
  – Notice of privacy practices
  – Access of individuals
  – Minimum necessary
  – Authorizations
• Most common Security Rule deficiencies
  – Risk analysis
  – Media movement and disposal
  – Audit controls and monitoring

OCR Audit Program Phase 1

• Most common cause for deficiency
  – Entity unaware of the requirement
• Other causes
  – Lack of application of sufficient resources
  – Incomplete implementation
  – Complete disregard
OCR Audit Program Phase 2

• Audit Program Phase 2 (originally scheduled for 2014-15)
  – 1200 CEs in audit pool
  – 550-800 CEs to be selected for online “pre-survey”
  – 350 CEs to be audited in 2 rounds
  – 50 BAs to be audited
• What does the delay mean?

OCR Audit Program Phase 2

• Audits to be conducted primarily by OCR staff
• Targeted areas of compliance
• Desk audit approach
• 2 weeks to produce documentation
• Some on-site visits
• CEs to produce list of BAs
How to Conduct an Assessment

• Follow OCR Audit Protocol

<table>
<thead>
<tr>
<th>Section</th>
<th>Established Performance Criteria</th>
<th>Key Activity</th>
<th>Audit Procedures</th>
<th>Implementation Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.308</td>
<td>§164.308(a)(1): Security Management Process §164.308(a)(1) (ii)(a) - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity,...</td>
<td>Conduct Risk Assessment</td>
<td>Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and avail...</td>
<td>Required</td>
</tr>
</tbody>
</table>

How to Conduct an Assessment

• Keep in mind published OCR Audit Protocol has not been updated for HITECH Final Rule

• Selection of subsidiaries and service lines

• Consider expanded review
  - Inventory documents
  - Physical walk-throughs, interviews
  - Employer-sponsored group health plan
  - Additional questions
How to Conduct an Assessment

• Consider internal self-review v. independent mock audit
• Consider attorney-client privilege
• Watch out for:
  – Insufficient or nonexistent Risk Analysis
  – Freshly minted, but unimplemented policies

Additional Questions to Ask

• Who’s on the team?
• Hybrid entity, OHCA and ACE statuses
• Cyber liability coverage
• Use of OCR guidance and resources
• OCR complaint/closure letter – documentation of response
• Breach log match up with individual and OCR notices
• Documentation of BA issuing breach notices
• Inclusion of medical devices in risk assessment
Additional Questions to Ask

- Due diligence in transactions
- Vendor screening due diligence
- Off-shore data
- Return of PHI at termination of contracts
- Other - PCI DSS, FDCPA, TCPA, state law

Margaret Marchak
SVP & Chief Legal Officer
Hartford HealthCare Corporation
One State Street, Suite 19
Hartford, CT 06103
margaret.marchak@hhchealth.org

Elizabeth Callahan-Morris
Shareholder
Hall, Render, Killian, Heath & Lyman, PLLC
201 West Big Beaver Rd., Suite 1200
Troy, MI 48084
(248) 457-7854
ecallahan@hallrender.com