Are You Ready for an OCR Audit?

Tom Walsh, CISSP
Tom Walsh Consulting, LLC
Overland Park, KS

What would you do?

Your organization received a certified letter sent from the Office for Civil Rights (OCR) to your CEO stating that the organization is being audited. Included with the letter is a list of requested documentation that needs to be sent within 15 business days.

• Do you have everything you need to respond to the document request and pass an audit?
• How confident are you that you will pass an audit?

Session Objectives

Upon successful completion of today's session, participants should be able to:

1. Identify the three types of OCR audits
2. Explain the type of documentation that could be needed prior to and during an audit
3. Leverage the HIPAA Audit Program Protocol, as a way to evaluate compliance
### Introduction – Tom Walsh

- Certified Information Systems Security Professional (CISSP)
- 11 years – Tom Walsh Consulting (tw-Security)
- Co-authored four books on security
- Former information security manager for large healthcare system in Kansas City, MO
- A little nerdy, but overall, a nice guy 😊

---

### Preparing for an Audit from the Office for Civil Rights (OCR)

---

### Timeline of Compliance Audits

<table>
<thead>
<tr>
<th>Date</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008 – 2009</td>
<td>CMS HIPAA Compliance Reviews</td>
</tr>
<tr>
<td>2012</td>
<td>HIPAA Security audits conducted by KPMG</td>
</tr>
<tr>
<td>June 2012</td>
<td>HIPAA Audit Program Protocol released</td>
</tr>
<tr>
<td>November 2012</td>
<td>Medicare EHR incentive program audits</td>
</tr>
</tbody>
</table>
Three Types of OCR Audits

1. **Investigation**
   - **Trigger**: Reported breach or patient complaint

2. **Random (HIPAA Compliance)**
   - **Trigger**: Not sure how entities get “selected”

3. **Meaningful Use**
   - **Trigger**: Entity received incentive money

---

**Investigation Audits**

- Focused audits that are event driven
  - Incident or breach
  - Compliant from patient
  - Whistleblower report
- Audit scope may widen if there is evidence of willful negligence
- Settlement results are typically:
  - Penalties or fines
  - Corrective Action Plan (CAP)
Investigation – OCR Audits

Samples of the evidence needed:
- Policies and procedures that were in place at the time of the incident or breach
  - OCR will examine the meta data
  - Date on documents must be before the letter is received
- Audit logs or audit reports
- Training content and records
- Agreements or forms signed by the worker(s)
- Emails

What is the retention requirement for HIPAA compliance?

Investigation – OCR Audits

Corrective Action Plans (sample)
- Examination of policies and procedures
- Implementation of revised policies and procedures
- Education or training of the workforce
- Risk management
- Annual reports to the OCR (from 1 to 3 years)

Investigation – OCR Audits

OCR has levied fines and corrective action plans against more than 20 organizations:
- Idaho State University ($400,000)
- Alaska Department of Health and Social Services ($1.7 million)
- Blue Cross and Blue Shield of Tennessee ($1.5 million)
- UCLA Health System ($865,000)
- Massachusetts General Hospital ($1 million)
- Cigna Health ($4.3 million)
- Rite Aid ($1 million)
- CVS/pharmacy ($2.2 million)
- Phoenix Cardiac Surgery ($500,000)
- Providence Health & Services ($100,000)
- The Hospice of North Idaho ($50,000)
Random Audits

Random – OCR Audits #1

- **February 2009** – The Department of Health and Human Services (HHS) through the Office for Civil Rights (OCR) is mandated (HITECH Act Section 13411) to provide periodic audits to make sure that covered entities and business associates comply with the requirements of HIPAA privacy and security.

- **On June 10, 2011**, HHS awarded to KPMG a $9.2 million contract to create an audit protocol and then conduct random audits as part of the pilot program.

Random – OCR Audits #2

- **By December 31, 2012** – 115 audits were conducted by KPMG.

- **Fiscal year 2014** – Start of a permanent audit program.

  “OCR officials also indicated that business associates, as well as covered entities, will be audited in the permanent program because they’re liable for HIPAA compliance under the HIPAA Omnibus Rule.”

  “A major weakness found during the pilot audit program, as well as through OCR breach investigations, has been a lack of thorough risk analysis, he added.”

  [Leon Rodriguez, director of the Department of Health and Human Services’ Office for Civil Rights as quoted in an article]
HIPAA Audit Program Protocol

Three components:

1. Privacy
2. Security
3. Breach Notification

“OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.”

Source: HHS website [http://ocrnotifications.hhs.gov/hipaa.html](http://ocrnotifications.hhs.gov/hipaa.html)

---

Missing from the Protocol?

- Tablet
- Smartphone
- Mobile devices
- Personally-owned devices
- Portable media
  - External hard drives and USB thumb drives
- Data loss prevention
- Data leakage
- Change control
- Configuration management
- BYOD
- Mobile device management
- Wireless networks
- Texting
- Secure messaging
- Web portal
- Secure website (https)
- Router, switch, firewall
- Networking scans
- Penetration testing
Also Missing…

- Biomed or Biomedical Devices
- Cloud
- Telecommute  
  - (such as remote coding and remote transcription)
- Telemedicine
- Teleradiology
- Social Security Numbers
- Software licensing (illegal software)
- Payment Card Industry Data security Standard (PCI DSS)

Audit Test Procedures

- For each criteria, there are typically three stated measures within the audit procedures:
  1. “Inquire of management...” (Perception)
  2. “Obtain...” some type of document (Policy)
  3. “Observe...” validate the safeguard and control is being followed (Practice)

- The three “P’s” need to align:
  1. Perception
  2. Policy
  3. Practice

Audit Test Procedures

A common “Audit Procedure” that would pertain to standards, policies, procedures, plans or any other forms of documentation...

Determine if the covered entity's formal or informal policy and procedures have been updated, reviewed, and approved and on a periodic basis.

1. Updated
2. Reviewed
3. Approved
Audit Test Procedures

For any of the 22 Addressable Implementation Specifications of the HIPAA Security Rule...
the same phrase is repeated:

*If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so*

*This needs to be documented in your book of evidence*

Create a “Book of Evidence”

- Proof of compliance - required by HIPAA
  - Identify and fill the gaps
- Minimize the time required to respond to a request for documentation
  - Once you are notified, the clock is ticking (15 days)
- Avoid making a bad first impression
  - Perception is the only reality
  - Being disorganized does not make a good impression on the OCR auditor

Create a “Book of Evidence”

- Two types of documentation in the book of evidence:
  - In response to the audit notification letter *(see additional handout)*
  - During the fieldwork – while the auditors are onsite *(see additional handout)*
What Drives the Audit Agenda?

- Prior audit findings from other OCR audits
- Reported breaches to HHS and common weaknesses that plague all of healthcare
- Your own policies
  - “Say what you do. Do what you say.”
- Your risk analysis and remediation plan

Let's learn from others…

CMS Audit Reports 2008 – 2009

Seven common areas of concern
1. Risk Assessment
2. Currency of Policies and Procedures
3. Security Awareness and Training
4. Workforce Clearance
5. Workstation Security
6. Encryption
7. Business Associate Contracts and Other Arrangements

CMS Audit Reports 2012

Source: 2012 HIPAA Privacy and Security Audit, Linda Sanchez, OCR Senior Advisor, Health Information Privacy Lead, HIPAA Compliance Audits
Meaningful Use

Meaningful Use – Stage 1

Objective:
Ensure adequate privacy and security protections for personal health information

Measure:
Conduct or review a security risk analysis in accordance per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

Meaningful Use, Stage 1 – Audits

Protect Electronic Health Information
(Core #14 – Hospitals; Core #15 - Eligible Professionals)

“Proof that a security risk analysis of the certified EHR technology was performed prior to the end of the reporting period (i.e. report which documents the procedures performed during the analysis and the results of the analysis). If deficiencies are identified in this analysis, please supply the implementation plan; this plan should include the completion dates.”
“OCR conducts audits for HIPAA privacy and security rule compliance. Providers in the CMS EHR incentive programs may also receive a random audit from CMS to determine if they actually conducted the security risk analysis and implemented adequate safeguards.”

Source: Guide to Privacy and Security of Health Information, released in May 2012
What does the ONC say about, “Risk Analysis?”

<table>
<thead>
<tr>
<th>Security Risk Analysis Myths and Facts</th>
<th>Fact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Myth</strong></td>
<td><strong>Fact</strong></td>
</tr>
<tr>
<td>The security risk analysis is optional for small providers.</td>
<td>False. All providers who are “covered entities” under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.</td>
</tr>
<tr>
<td>Security installing a certified EMR fulfills the security risk analysis MU requirement.</td>
<td>False. Even with a certified EMR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EMR.</td>
</tr>
<tr>
<td>My EMR vendor took care of everything I need to do about privacy and security.</td>
<td>False. Your EMR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EMR product. However, EMR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.</td>
</tr>
<tr>
<td>I have to outssource the security risk analysis.</td>
<td>False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guide is intended to help organizations in identifying and implementing the most effective and appropriate safeguards to secure ePHI.</td>
</tr>
<tr>
<td>A checklist will suffice for the risk analysis requirement.</td>
<td>False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.</td>
</tr>
<tr>
<td>There is a specific risk analysis method that I must follow.</td>
<td>False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guide is intended to help organizations in identifying and implementing the most effective and appropriate safeguards to secure ePHI.</td>
</tr>
</tbody>
</table>

False: Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHIs hardware and software and devices that can access your EHR data (e.g., your laptop computer, your practice manager’s mobile phone). Remember that you are only complying with HIPAA when you are following the Security Rule. Do not rely on a written plan to follow the Security Rule. Any actions must be documented. For more on assessing your security practices, please see http://healthit.hhs.gov/tutorials/questionnaire/HealthIT_gov__privacy__security.html#173. |

False: The EMR incentive program requires addressing any deficiencies identified during the risk analysis during the reporting period. |

False: Perform the full security risk analysis as you adopt an EMR. Each year or when changes to your practice or electronic systems occur, review and update the plan or analysis for changes to risk.
Looking Ahead… MU Stage 2

For security…
Essentially the same requirement as Meaningful Use Stage 1, except –
This time the risk analysis must address, encryption / security of “data at rest”

Meaningful Use – Stage 2

Objective:
Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities

Measure:
Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP’s risk management process.

Threats to “Data at Rest”

- Unauthorized access to a database or files on a server, SAN, or NAS
- Theft or loss of media (tapes, CDs, DVDs, USB drives, external hard drives, memory cards, etc.) or mobile devices (laptops, tablets, smartphones, etc.) that store PHI or other confidential information
- Hacking of the database or hijacking of a database
- Reuse or disposal of a device which may contain PHI
- Unauthorized access to confidential information stored on a workstation, laptop, tablet or smartphone
- Malicious code (virus, worm, etc.)
- Deletion of data or files (unintentionally or intentionally)
- Encryption key management (user forgets how to unencrypt data) or media is no longer readable (hardware failure or old media format)
Other Things to Consider

HIPAA Compliance

• Business Associates
  – Omnibus Rule: Compliance by September 23, 2013
  – Small business associates – Are they compliant?
  – No audit protocol yet for business associates

• Physician group practices and clinics
  – Hospitals are buying up physician practices
  – Immediately assume the liability for noncompliance with Meaningful Use and HIPAA

Resources

• HIPAA Audit Program Protocol
  http://ocrnotifications.hhs.gov/hipaa.html

• Article:
  HIPAA Audits: More to Come in 2014
  – By Marianne Kolbasuk McGee, September 23, 2013

• Presentation:
  6 Steps to Showing HIPAA Privacy/Security Compliance