Disclosure:

The information presented is not meant to constitute legal advice. Consult a healthcare attorney for any advice on any specific HIPAA incident.
Topics and Objectives

1. Introduction to Audit types
2. Analyze steps required: OCR HIPAA Audit processes
3. Present tips to respond Accurately and Efficiently
4. Demonstrate Tools & Techniques to help assess your ability to respond
5. Lessons Learned from past Audits
Often begins with a Letter

Note: The Audit Program, mandated by Section 13411 of the ARRA of 2009, required OCR to periodically evaluate Covered Entities and Business Associates compliance with the HIPAA Privacy and Security Rules.
Audits are primarily a compliance improvement activity. OCR will review and analyze information from the final reports. The aggregated results of the audits will enable OCR to better understand compliance efforts with particular aspects of the HIPAA Rules.
Audit Types & Approaches

OCR Desk Audit
OCR Field Audit
Civil Liability Audit
Audit Checklists
Mock Audit
Outsourced Audit

Audits are based on all HIPAA Rules: i.e. Privacy, Security and Breach Notification
OCR Compliance Audits – Sample Timeframe

Estimated Elapsed Time

- **1 Day**
  - Notification Letter sent to Covered Entity

- Minimum of 10 Days
  - Receiving and Reviewing Documentation and Planning the Audit Field Work

- 5 – 10 Days
  - Onsite fieldwork

- 30+ Days
  - Draft Audit Report

- 10 Days
  - Covered Entities Review and Comment on Draft Audit Reports

- 30+ Days
  - Final Audit Report

- Dependent on completion of fieldwork

“HIPAA compliance is not a destination, it's a journey.”

Image credit: Department of Health & Human Services
OCR Audit - Triggers

- Random Selection - Desk Audits
- Past HITECH MU Participation
- Patient Complaints
- Class Action Lawsuits
- HIPAA Violations – Breach Notification Protocol
- MACRA/MIPS Reporting/Compliance
- Cyber-Insurance Liability Coverage
If it isn’t documented, It didn’t happen!

What?
- Security Risk Assessment

Where?
- Practice: Policies & Procedures

How?
- Automated User Monitoring
The Desk Audit

CMS/OCR Initiated
What gets Examined?

1. Violations of simplest standards/documentation processes
2. Can you account for **ALL** your Business Associates (BA)
3. Year-to-Year improvements in processes: Addressing Gaps
4. Not planning to “air less than clean white laundry”
5. BA audits will be reviewed on Security Rule and breach response
6. Onsite for both CE & BA
7. BA should review CE audit info, it will basically be the same
### Audit Focus: By the Book

<table>
<thead>
<tr>
<th>Requirements Selected for Desk Audit Review</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy Rule</strong></td>
</tr>
<tr>
<td>Notice of Privacy Practices &amp; Content Requirements [164.520(a)(1)&amp;(b)(1)]</td>
</tr>
<tr>
<td>Provision of Notice – Electronic Notice [164.520(c)(3)]</td>
</tr>
<tr>
<td>Right to Access [164.524a(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]</td>
</tr>
<tr>
<td><strong>Breach Notification Rule</strong></td>
</tr>
<tr>
<td>Timeliness of Notification [164.404(b)]</td>
</tr>
<tr>
<td>Content of Notification [164.404(c)(1)]</td>
</tr>
<tr>
<td><strong>Security Rule</strong></td>
</tr>
</tbody>
</table>
After review of submitted documentation:

- Draft findings are shared with the CE
- CE may respond in writing

Final Audit Reports will:

- Describe how the Audit was conducted
- Present any findings, and
- Contain any written CE 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 reviewed through the Audit
## Contents of a Desk Audit - Drivers

<table>
<thead>
<tr>
<th>Question</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are the privacy and security measures comprehensive and current?</td>
<td>✔</td>
</tr>
<tr>
<td>Are the right policies and procedures in place?</td>
<td></td>
</tr>
<tr>
<td>Is there a Security Rule risk assessment?</td>
<td></td>
</tr>
<tr>
<td>Are there proper training programs for employees?</td>
<td></td>
</tr>
<tr>
<td>Are the business associate relationships properly documented?</td>
<td></td>
</tr>
<tr>
<td>Are the subcontractors properly being engaged in the context of HIPAA regulations?</td>
<td></td>
</tr>
<tr>
<td>Is there good coordination about what’s in place between the privacy officer, the in-house legal team, and external team? Are they ready to respond if and when they get the audit request?</td>
<td></td>
</tr>
<tr>
<td>Are all personnel, especially those who work in a compliance role, carefully monitoring for any emails or letters that come in from OCR?</td>
<td></td>
</tr>
<tr>
<td>Do the personnel know who the compliance officers are, or the designated health information privacy and security officials are? The OCR sends out a communication to confirm that it has the correct contact information so that it can identify the correct mailing address and email address.</td>
<td></td>
</tr>
</tbody>
</table>
Field Audit

OCR Auditor On-Site
What to have Prepared

Security Risk Assessment
Policies & Procedures
User Monitoring
Gaps & Vulnerabilities
Action Plan
Disaster Recovery Plan
Education Plan

You will be given a chance to correct any discrepancies
Recommendation: Conduct a Mock Audit

• Using the published OCR Audit Protocol, conduct an internal, or solicit and external, Mock Audit
  • Prepare an Audit Response Team
  • Follow the same process steps as OCR
  • Use a local or secure cloud-based portal to submit documents to a review panel
  • Follow the 2016 Desk Audit Guide as your document request criteria:
• Conduct and critique in-person interviews
• Use activity scanning tools to assess ePHI vulnerabilities
• Update mitigation pathways for HIPAA Risk Analysis
Best Practices to Prepare for an OCR HIPAA Audit

1. Prove you’ve set HIPAA Policy and Procedure Boundaries
2. Focus on PHI/ePHI
3. Conduct: Security Risk Assessment (SRA)
4. Develop an Incident Response Plan
5. Know Your Users (Employees and BAs)
6. Identify High-Risk Assets (Technical and Non-Tech)
7. Don’t skimp on Business Associate Agreements
8. Implement Ongoing Training/Education
Civil Liability Audit

Lawsuit Procedures
Civil Liability Audit Prompts

• Think: Patient Instigated Investigation
  • Ex: Delaware Online Privacy and Protection Act 2016
  • Ex: California Consumer Privacy Act – 2018
    • Know what personal data is being collected about them.
    • Know whether their personal data is sold or disclosed and to whom.
    • Say NO to the sale of personal data.
    • Access their personal data

• Many States to follow: 17 States currently
• Request for Information – Response required within 15 days
Audit: Findings to Date

- Lack of Business Associate Agreements
- Incomplete or Inaccurate Security Risk Analysis
- Not performing an organization-wide risk analysis
- Lack of Transmission Security - No encrypting PHI on devices
- No Patching of Software
- Third-party disclosure of PHI
- Improper disposal of PHI
- Employees disclosing information
- Employees illegally accessing patient files
- Lost or stolen devices
- Lack of training – No Incident Response Plan

Settlements leave money to allow you to fix things...
BECAUSE PRIVACY MATTERS

SPHER™ provides a scalable, SaaS-based compliance and risk management tool that utilizes AI technology to monitor 100% of daily user activity to detect potential breaches of sensitive patient protected health records.

Audit
Alert
Manage

WWW.SPHERINC.COM
info@spherinc.com
The Solution: PHI Cybersecurity Simplified

SPHER™ provides a scalable, SaaS-based compliance and risk management tool that utilizes AI technology to monitor 100% of daily user activity to detect potential breaches of sensitive patient health records.
Case Study: Surviving an OCR Audit

OCR initiated audits specific to User Access & System Monitoring Fault. Major HIPAA fines and penalties avoided via SPHER rollout across all MSO Covered Entities.

- SPHER™ +
  - Security Risk Assessment
  - Harris CareTracker™
  - Internal P&S Training
  - Ongoing Education

- SPHER Monitors:
  - 60+ Clinics,
  - 1200+ employees
  - 120+ physicians
  - Now monitors 100% of all daily ePHI activities

- 17+ Subsequent follow-up audits. Clean bill of health across all businesses

- SPHER was the key component of the Argus privacy & security procedures overhaul
  - Instilled a Culture of Compliance
  - CEO and CISO provide references for SPHER

$1.7M in OCR fines avoided
Thank You!
&
Stay Secure

For more information:
Ray.Ribble@SPHERINC.com
Linkedin.com/in/Raymond-F-Ribble
Tel: (310) 602-5140  x5513
www.spherinc.com