OCR Launches Phase 2 HIPAA Audits for Covered Entities and Business Associates: Are You Ready?

Developing, Ensuring and Documenting HIPAA and HITECH Privacy and Security Compliance; Lessons Learned From Phase 1

TUESDAY, MAY 17, 2016
1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today’s faculty features:

Bruce D. Armon, Partner, Saul Ewing, Philadelphia

Karilynn Bayus, Vice Chair, Health Care Practice Group, Saul Ewing, Philadelphia

Samuel C. Cohen, Esq., Arent Fox, Washington, D.C.

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Tips for Optimal Quality

Sound Quality
If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial 1-866-819-0113 and enter your PIN when prompted. Otherwise, please send us a chat or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality
To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.
Continuing Education Credits

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 35.
Phase 2 HIPAA Audits for Covered Entities and Business Associates

Are You Ready for Your Audit?
What will be covered today?

- Pre-Phase II HIPAA Background
- Phase 2 HIPAA Audits
- Preparing for an OCR Audit
- Conducting a Self-Audit
- Takeaways
Pre-Phase II HIPAA Background

How did we get here?
HIPAA – General Overview

  - Privacy Rule finalized in 2000; Security Rule finalized in 2003
  - In 2009 Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act of 2009, which made changes to HIPAA, including a new breach notification requirement
  - The HITECH final regulations have been in effect since September 23, 2013
Role of the Office for Civil Rights (OCR)

- OCR is responsible for overseeing covered entities’ and business associates’ compliance with the Privacy Rule, Security Rule and Breach Notification Rule
- Authority to investigate and resolve complaints
- Section 13411 of the HITECH Act requires OCR to conduct periodic audits to ensure HIPAA compliance by covered entities and business associates
HIPAA Phase 1 Audits (Pilot Program)

- Conducted in 2011 and 2012
- 115 covered entities audited – no business associates
  - Health plans, health care providers and health care clearinghouses of varying sizes selected
- All Phase 1 audits included a site visit and resulted in an audit report
Move Toward Phase 2

- In 2013 OCR conducted an evaluation program to assess Pilot Program’s effectiveness.

- In a September 2015 Report, the HHS Office of Inspector General (OIG) criticized OCR for not having fully implemented the HITECH-required audit program.
  - OIG recommended implementation of a permanent audit program for privacy compliance.
  - In response, OCR announced Phase 2 audit program beginning in 2016.
HIPAA Phase 2 Audits – What to Expect
Scope - Auditees

- Every covered entity and business associate is eligible
- OCR is initially obtaining and verifying contact information to create potential auditee pool
- Questionnaire designed to gather data about the potential auditees
  - Criteria include size, affiliation with other healthcare organizations, types of entity, public/private status, geography
  - Organizations with an open investigation or compliance review are excluded
- Random sampling selection
- Failure to respond does not exempt the entity from the audit pool
Scope – Subject Matter

- Privacy, Security and Breach Notification Rules
  - On-site audits will be more comprehensive than desk audits
- Auditees notified of the subject(s) of their audit in a document request letter
- No state law compliance
Timelines

- Verification of contact information underway
- In coming months, first auditees will be notified, including requests for documents
- 10 business days to respond to draft findings
- Final audit report within 30 business days of OCR’s receipt of response
- Desk audits to be completed by December 2016; on-site audit timing unclear
Phase II Audit Process

- First wave of audits are desk audits
  - Only digital submission - through OCR secure portal
  - Draft findings and response period
  - Final report

- Second wave are on-site audits
  - Draft findings and response period
  - Final Report

- Post-Audit: Potential compliance review of “serious” issues
Preparing for an OCR Audit
Preparing for an OCR Audit

1. Check for Communications from OCR
2. Develop an Audit Response Plan
3. Assess Existing HIPAA Policies and Procedures
4. Identify (and Address) Risk Areas Identified by OCR
5. Locate HIPAA-Required Documentation
Check for Communications from OCR

- OCR will be sending emails to CEs & BAs:
  - Verify and/or obtain contact information
  - Pre-audit questionnaires
  - Audit notification letters

- Audit-related emails to be sent from: OSOCRAudit@hhs.gov

- Timeframe:
  - CEs already may be receiving audit notification letters
  - BAs expected to begin receiving audit letters in June/July
Check for Communications from OCR

- Determine personnel most likely to receive OCR emails
- Establish process to ensure that audit-related emails are identified and received by proper personnel
  - Continually check email inboxes
  - Confirm emails are not being diverted to junk or spam email folders
  - Automatically forward emails from OCR’s audit email address to a designated individual
- OCR expects all entities to be checking for audit-related emails
Develop an Audit Response Plan

- Implement an audit response plan BEFORE receiving an audit notification letter

- Identify key individuals and support for audit response:
  - Who will coordinate the response?
    - Privacy Officer and/or Security Officer?
    - General Counsel? Outside counsel?
  - What other personnel will assist with the response?
  - What resources are available for responding to the audit?

- Identify and locate all potentially relevant documents
Assess Existing HIPAA Policies and Procedures

- Review and update policies and procedures
- Identify existing compliance gaps
- Address compliance gaps
  - Implement changes to address gaps
  - Revise written policies and procedures
Assess Existing HIPAA Policies and Procedures

- Use existing guidance documents and risk assessment tools
  - OCR Security Series
  - National Institute of Standards and Technology (NIST) Publications
Identify (and Address) Risk Areas Identified by OCR

- Findings from Phase 1 HIPAA Audits
  - Privacy Rule, Breach Notification Rule, and Security Rule issues
  - Most common cause for identified issue?
    = Entity unaware of the requirement
Privacy Rule – Noted Issue Areas

- Uses and disclosures of PHI
  - Business Associates, Identity Verification, Minimum Necessary, Authorizations, Deceased Individuals, Personal Representatives, Judicial and Administrative Procedures, Group Health Plan Requirements
- Notice of Privacy Practices
- Administrative requirements
  - Policies and procedures, training, complaints, sanctions
- Individual access to PHI
- Right to request privacy protection for PHI
Identify (and Address) Risk Areas Identified by OCR

- Security Rule – Noted Issue Areas
  - Two-thirds of entities did not have a complete and accurate risk assessment
  - Other identified issues
    - Risk analysis
    - Access management
    - Security incident procedures
    - Contingency planning and backups
    - Workstation security
    - Media movement and destruction
    - Encryption
    - Audit controls and monitoring
    - Integrity controls
Recent Resolution Agreements

- Lack of enterprise-wide risk analysis
- Not implementing controls to address weaknesses identified by risk analysis
- Lack of business associate agreements
**Identify (and Address) Risk Areas Identified by OCR**

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Settlement</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2016</td>
<td>New York Presbyterian Hosp.</td>
<td>$2.2 million</td>
<td>Filming of patients without patient authorization</td>
</tr>
<tr>
<td>April 2016</td>
<td>Raleigh Orthopaedic Clinic, P.A.</td>
<td>$750K</td>
<td>Disclosure of PHI of 17,300 patients to potential business partner without written BA Agreement</td>
</tr>
<tr>
<td>March 2016</td>
<td>Feinstein Institute for Medical Research</td>
<td>$3.9 million</td>
<td>Theft from car of unencrypted laptop with PHI of 13,000 patients; insufficient security management process</td>
</tr>
<tr>
<td>March 2016</td>
<td>North Memorial Health Care System</td>
<td>$1.55 million</td>
<td>Disclosure of PHI involving 290,000 patients to BA without BA Agreement; no system-wide risk analysis</td>
</tr>
<tr>
<td>February 2016</td>
<td>Complete P.T., Pool &amp; Land Phys. Therapy, Inc.</td>
<td>$25K</td>
<td>Posting of patient testimonials, including names and full face photographs, without valid patient authorization</td>
</tr>
<tr>
<td>December 2015</td>
<td>University of Washington Medicine</td>
<td>$750K</td>
<td>PHI of 90,000 individuals accessed after download of email attachment with malware; risk assessments for some affiliated entities not conducted properly</td>
</tr>
<tr>
<td>Nov. 2015</td>
<td>Triple-S Mgmt. Corp.</td>
<td>$3.5 million</td>
<td>Disclosure of PHI to vendor without BA Agreement; did not conduct risk analysis and implement privacy/security safeguards; minimum necessary violations (re: mailings)</td>
</tr>
</tbody>
</table>

A complete list of Resolution Agreements is available at: [http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html](http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html).
Locate HIPAA-Required Documentation

- Business Associate Agreements
  - Agreements
  - Listing of Contact information for each BA ([http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html](http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html))
- Policies and procedures
- Training materials (and proof training was completed)
- Breach logs
- Explanations re: why addressable security rule specifications have not been implemented (if applicable)
Locate HIPAA-Required Documentation

- Other internal HIPAA audit activity?
  - Remember: if it is not in writing, it does not count

- Make sure documentation is in a format that easily can be uploaded to the OCR web portal
Conducting a Self-Audit
Assess Existing HIPAA Policies and Procedures

- Phase 2 Audit Protocol
  - Revised April 2016
  - 180 areas of inquiry
    - Phase 1 Audit Protocol = 165 areas of inquiry
  - Includes specific questions related to each HIPAA requirement
  - Covers Privacy Rule, Breach Notification Rule, and Security Rule
Privacy Issues

- Identify a point person, and a back-up point person
- Privacy/Security Breach Notification Committee across the organization
- Gather and review your HIPAA privacy policies and forms
  - Are they available in an accessible and comprehensive way to your workforce?
  - When were they last updated? Is the most recent document identified and dated?
  - Are your forms (e.g., NPP) consistent with your policies?
  - Are the policies appropriate and comprehensive to your organization?
  - Do you need external review under attorney/client privilege?
Privacy Issues (cont’d)

- Spot check your workforce
- Ensure you have an inventory of all of your BAAs
- Update and create new policies and procedures as necessary. Conduct workforce training
Security Issues

- Gather and review your security policies and procedures
  - Do they ensure the confidentiality, integrity and availability of ePHI?
  - Do they protect against reasonably anticipated threats or hazards to the security or integrity of ePHI?
  - Do they protect against reasonably anticipated impermissible uses of disclosure of ePHI?
  - Is each required standard met and is each addressable standard addressed?
- Involve your IT department
- Do you need an external consultant?
Security Issues (cont’d)

- Ensure a recent, accurate and thorough risk analysis has been done
  - Importance of the risk analysis
- Confirm risk management policies and procedures have been implemented and are appropriate to the risk assessment
Breach Notification and Reporting procedures

- Ensure Omnibus-Updated policies and procedures are in place
- Has workforce been trained?
- Can your workforce identify an inappropriate use or disclosure of PHI? Do they know to whom they should report?
- Check your organization’s breach and “incident” logs
  - Are risk assessments available for each “incident”?
The Audit Protocol

- The HIPAA Audit Protocol is a road map for self-auditing: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
The Audit Protocol (cont’d)

- Audit Type: Privacy, Security, Breach
- Section: CFR cite
- Key Activity
- Established Performance Criteria
- Audit Inquiry
- Requested/Addressable (for Security Rule only)
Audit Inquiry Examples: Privacy Rule

- Deceased Individuals
- Personal Representatives
- Disclosure by Whistleblowers
- Business Associate Agreements
Audit Inquiry Examples: Privacy Rule (cont’d)

- Authorizations
- Facility Directories
- Research
- Minimum Necessary
Audit Inquiry Examples: Privacy Rule (cont’d)

- Fingerprinting
- Verification
- NPP
- Rights to Access
- Documentation
- Training
Audit Inquiry Examples: Privacy Rule (cont’d)

- Safeguards
- Sanctions
- Policies and Procedures
Audit Inquiry Examples: Security Rule

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
Audit Inquiry Examples: Security Rule (cont’d)

- Contingency Plan
- Evaluation
- Facility Access Controls
- Workstation Security
- Access Control
- Encryption
Audit Inquiry Examples: Breach

- Complaints
- Risk Assessment
- Unsecured PHI
- Notifications
Next Steps; Cleaning Up. Which do you prefer?
Takeaways

- HIPAA compliance not going away
- Public announcements and settlement payments are on the rise
- You have the government tool kit for how to be successful
- Regular and routine oversight and updates are essential
- Don’t forget about state laws!
- Privacy and security issues are broader than HIPAA