Preparing for HIPAA Audits in 2016 and Beyond

Cynthia A. Haines, Esquire
Post & Schell, PC
17 North 2nd Street, 12th Floor
Harrisburg, PA 17101
717-612-6051
Chaines@postschell.com
Background Phase 1 of HIPAA Audit Program

- HITECH requires HHS to perform periodic audits of:
  - Covered entity
  - Business associate
  - For compliance with HIPAA Privacy, Security, and Breach Notification Rules
Background Phase 1 of HIPAA Audit Program

- OCR established a pilot audit program
- OCR developed a protocol, to measure the efforts of 115 covered entities
- OCR instituted a formal evaluation of the effectiveness of the pilot audit program
Phase 2 of HIPAA Audit Program Objectives

- To examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities

- Get out in front of problems before they result in breaches

- Broadly identify best practices gleaned through the audit process and will provide guidance targeted to identified compliance challenges
DATE

Contact Person's Name
CEBA Name
Address
City, State ZIP

Dear Contact:

This is an automated communication from the Office for Civil Rights (OCR).

According to our records, you are the primary contact OCR should use to reach Entity Name regarding its potential inclusion in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program. We are attempting to verify this email address.

Please respond within fourteen (14) days as instructed below to either confirm your identity and email address or instead provide updated primary and secondary contact information.

If you ARE the primary contact for this organization, please select the following link YES. Once the link is selected, a browser window will open and your response will be recorded.

If you ARE NOT the primary contact for this organization, please select the following link NO. Once the link is selected, a browser window will open and your response will be recorded.

Thank you for your cooperation. If we do not receive a response from you we will use this email address for future communications with this entity. Failure to respond will not shield your organization from selection.

If you have questions or comments regarding this message, you may contact us at OCRAudits@hhs.gov.

Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr
WHO

• Every covered entity and business associate is eligible for an audit

• OCR is identifying pools of covered entities and business associates that represent a wide range of health care providers, health plans, health care clearinghouses and business associates
HOW

- Criteria-
  - Size of the entity
  - Affiliation with other healthcare organizations
  - The type of entity
  - Its relationship to individuals
  - Public or private
  - Geographic factors
  - Present enforcement activity with OCR
Selection Process

- Basic Pre-screening questionnaire
- List of each business associate with contact information
- Random sampling of the audit pool
- “If a covered entity or business associate fails to respond to information requests, OCR will use publically available information about the entity to create its audit pool. An entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.”
HOW

- Desk and onsite audits for both covered entities and their business associates
- Desk audits for covered entities
- Desk audits of business associates
- All completed by Dec, 2016
- The third set of audits-onsite. Some desk auditees may be subject to a subsequent onsite audit
Desk Audit

- Email notification of selection - team
- Provide documents and other data in response via OCR’s secure portal within 10 business days
- Fewer in person visits during these Phase Two
- Auditors will review documentation and share draft findings with the entity
- Auditees will have the opportunity to respond
- Final audit report within 30 business days after the auditee’s response
- Written responses will be included in the final audit report
On-Site Audit

- Notified via email of their selection for an onsite audit
- An entrance conference and provide more information about the onsite audit process and expectations for the audit
- Onsite audit will be conducted over three to five days onsite
- More comprehensive than desk audits and cover a wider range of requirements from the HIPAA Rules
- Entities will have 10 business days to review the draft findings and provide written comments
- Final audit report within 30 business days after response.
- Written responses will be included in the final audit report
Audit Protocol

- 300 pages!
- Reviews the policies and procedures adopted to meet “selected standards and implementation specifications” of the Rules
- Protocol is organized by Rule and regulatory provision
Communication with the Auditors

• Be responsive to the auditors.

• If you cannot meet a deadline, let the auditors know as soon as possible.

• If you have questions about the information being requested, ask the auditors for clarification.
Documentation

- Initial list of requested documentation provided by the audit letter may not be all-inclusive

- Auditors may request additional information necessary to complete the audit

- Provide only the information requested in the audit letter and ask questions about the audit if unsure of how to respond
Privacy/Security During the Process

- During the entire audit process, protect patient confidentiality
- De-identify patient information, per HIPAA requirements
- Do no talk about individual residents
- Be mindful of your surroundings if there is an on-site audit
- Do not want to face an OCR Compliance Investigation
OCR Guidance

- The guidance is extensive (and free)
- Publications available describing the audit process
- Publications available describing the type of information that must be provided
- Protocol specifically gives you OCRs checklist
Privacy and Security Risk Analysis

- Security Risk Analysis Tipsheet from CMS and OCR:

- OCR Guidance on Risk Analysis:
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
Audit Response Plan

• Build a foundational Privacy, Security and Breach Response Plan

• Solid documentation to support the effort in the event of an audit

• Defined procedure in place to manage the audit process

• Training and education of key personnel
Audit Response Plan

- Roles and responsibilities for each phase of the audit outlined

- Have an audit response fire drill where team members walk through all the steps that take place beginning with receipt of the Audit Letter

- Recognize and process Audit letters in a timely manner

- Produce documentation quickly
After an Audit

• “Audits are primarily a compliance improvement activity.”

• OCR will use the audit reports to:
  ▪ Provide technical assistance
  ▪ Assist with corrective action
  ▪ Develop tools and guidance to assist the industry in compliance

• Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to further investigate
Who Can See It

- Will not post a listing of audited entities or the findings
- Under the Freedom of Information Act (FOIA), OCR may be required to release information about audits
Questions?

Cynthia A. Haines, Esquire
Post & Schell, PC
17 North 2nd Street, 12th Floor
Harrisburg, PA 17101
717-612-6051
Chaines@postschell.com