U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

HIPAA Privacy, Security & Breach Notification Compliance Audits
Phase 2

October 19, 2016

Deven McGraw

Department of Health and Human Services

Office for Civil Rights

Division of Health Information Privacy

Status

- Desk audits of Covered Entities underway
- Basis of analysis *only the documents submitted in response to OCR's document request*
- Business Associate desk audits starting this fall
  - Selection pool largely BAs identified by CEs
- Comprehensive on-site audits of both CEs and BAs will begin in 2017

Topics

- Introduction
  - Phase II HIPAA Audit Program
  - Random Selection Process
  - Desk Audits vs. On-site Audits
- Desk Audit Mechanics
  - What to Expect
  - Subject HIPAA Controls
  - Document Request – Receipt and Response
  - Final Reports
  - Available Guidance

PHASE II Audit Overview

First phase 2012: comprehensive, on-site audits of 115 covered entities

Phase II:

- Includes both covered entities and business associates
- Over 200 audits total
  - Over 200 desk audits
  - Smaller number of comprehensive on-site audits

Phase II designed to

- Examine mechanisms for compliance
- Identify industry best practices
- Discover risks and vulnerabilities not surfaced through enforcement activities
- Enable us to get out in front of problems before they result in breaches

OCR Audit Goals

Audits primarily a compliance improvement activity to help OCR to

- better understand compliance efforts with particular aspects of the HIPAA Rules.
- determine what types of technical assistance OCR should develop
- develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches.

OCR will not post a listing of audited entities or entity-identified findings.

CE Selection Process

- Identified pools of wide range of CEs
- Sampling criteria included size, affiliations, location, public or private, etc.
- Health plans were divided into group plans and issuers and providers were further categorized by type, e.g.
  - hospital, practitioner, elder care/SNF, health system, pharmacy
- Ran a randomized selection algorithm that drew from each of the categories, resulting in 167 CEs.
- Finally, selected auditees checked for conflict of interests with the contractor supporting OCR in the audit process, as well as subjects of ongoing investigations. "Conflicted" auditees were replaced in kind.

Desk Audits Now, On-site Audits Later

- Covered entity desk audits underway: BA desk audits beginning in November.
- Desk audit scope limited to 7 controls drawn from the Security, Privacy, Breach Notification Rule Protocols
  - **CE on SR controls or PR & BNR**
  - **BAs on security and breach**
- On-site audits will begin in early 2017
- On-site audits will evaluate auditees against comprehensive selection of controls in protocols
- A desk audit subject may be subject to on-site audit

Desk Audit Expectations

Entities have 10 business days to provide responses

- Responses should contain the specified documentation--applicable policies, procedures, evidence of implementation
- Provide complete and relevant materials
- Refrain from submitting superfluous documentation! 10MB file size limitation

- The same rules and expectations apply to the BA auditees
- Over 20,000 BAs identified through CE listings

Document Requests & Responses

The CE document request

- Sent to selected auditees via email
- Comprised of two separate requests
  - one listing policies, procedures, and/or other related documentation to be provided
  - one requesting a list of all the CE's BAs
- Note that BA listings were required to be returned electronically, via email, to OCR within 10 business days
- All other items submitted using the secure online portal link provided in the notification email

Desk Audit Controls

Privacy Rule Controls	Notice of Privacy Practices & Content Requirements [§164.520(a)(1) & (b)(1)]
	Provision of Notice – Electronic Notice [§164.520(c)(3)]
	Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]
Breach Notification Rule Controls	Timeliness of Notification [§164.404(b)]
	Content of Notification [§164.404(c)(1)]
Security Rule Controls	Security Management Process -- Risk Analysis [§164.308(a)(1)(ii)(A)]
	Security Management Process -- Risk Management [§164.308(a)(1)(ii)(B)]

Desk Guidance

Element #	Audit Type	Section	Key Activity	Audit Inquiry
S2	Security	§164.308 (a)(1)(ii)(A)	Security Management Process -- Risk Analysis	Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits? Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits? Determine how the entity has implemented the requirements. Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated. Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate and determine whether the risk analysis or other documentation contains: • A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures

Guidance

Document Request List	Questions / Answers
Upload policies and procedures regarding the entity's risk analysis process. Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six (6) years prior to the date of receipt of notification. Consistent with 164.316(b)(2)(ii)-(iii), upload documentation from the previous calendar year demonstrating that documentation related to the implementation of this implementation specification is available to the persons responsible	Q; Can we submit documentation of an annual risk assessment performed by third party? A: Yes, a covered entity may use a business associate to conduct the risk analysis and the results may be submitted in response to S2 (1), Security Rule Risk Analysis. Q; If we recent conducted a risk analysis, but the report is in draft form - should we submit the draft, as well as the prior finalized risk analysis? A: Where entities are asked to provide documentation for a specified time period (e.g., current, previous calendar year, 6 years ago) they should submit documentation that reflects what is in place and in use during the time frame specified. Q: Can you please clarify the difference between S2 question 1 and 5? A: Question 1 is asking for the results of the risk analysis. Question 5 is asking for documentation that the risk analysis was conducted. Q: For the SR S2 Document request, is the request to upload documentation of CURRENT risk analysis results refering to 2015?

Desk Audit Reporting: Process

After review of submitted documentation:

- OCR will develop and share via email draft findings with the entity
- Entity may respond to draft findings – within 10 days; such written responses will be included in the final audit report
- Final audit reports will describe how the audit was conducted, present any findings, and contain entity responses to the draft findings
- 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 revealed through the audit

Audit Guidance

Posted Guidance for 2016 Desk Audits

- Selected protocol elements with associated document submission requests and related Q&As
- Slides from audited entity webinar held July 13, 2016
- Comprehensive question and answer listing

OCR Website:

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html