HIPAA
AUDIT GUIDE

**by Maggie Gloeckle
and Daniel J. Solove**

Table of Contents

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) includes national standards for the privacy of protected health information, the security of electronic protected health information, and breach notification to consumers.

HITECH also requires that periodic audits be performed of covered entities and business associates to ensure compliance with the HIPAA Privacy (45 CFR Part 160 and Subparts A and E of Part 164), Security (45 CFR Part 160 and Subparts A and C of Part 164) and Breach Notification Rule (45 CFR Part 164 Subpart D)

As of December 2016, according to the Office for Civil Rights (OCR) senior advisor Linda Sanches, there are more than 200 audits ongoing – 167 focused on providers and 48 focused on business associates.

OCR is looking for evidence that policies and procedures are being implemented.

Sanches has acknowledged that they are seeing two huge problems with implementation of risk analysis and risk management.[1]

In a recent article by Tammy Worth, published December 13, 2016, the first round of HIPAA audits by the US Department of Health & Human Services (HHS) Office for Civil Rights (OCR) found that providers are still not doing some of the most basic tasks required by the law.

More than half of those audited failed to complete a risk assessment, a main tenet of HIPAA. Many are not addressing weaknesses found in a risk analysis. And others still do not have required business associate agreements in place with vendors.[2]

---

[1] Source: http://www.healthcareitnews.com/news/ocr-onsite-hipaa-audits-coming-2017

[2] Source: http://www.renalandurologynews.com/hipaa-compliance/first-round-of-hipaa-audits-exposes-providers-weaknesses/article/578688/

Audit Phases

The audits are being conducted in two phases. Phase One was completed in December 2012 and began with a pilot program in 2011. The more recent Phase Two began in the fall of 2016.

Phase 1

In 2011, HHS Office of Civil Rights (OCR) established a pilot program to conduct assessments to determine the controls and processes that covered entities had put in place to comply with the Privacy, Security and Breach Notification rule.

OCR established a program and instructions that were used to assess 115 covered entities.

The Audits provided an opportunity to look at mechanisms for compliance, identify best practices, and discover risks and vulnerabilities that may not have previously been discovered through ongoing complaint investigations and compliance reviews.

Included in the audit were covered entities.

Covered entities ranged from covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses.

The pilot program was a three-step process:

1. Develop the audit protocols.

2. Test the protocols by performing a limited number of audits, of which the results would be used to perform the rest of the audits.

3. Complete the remaining audits using the revised protocols.

Phase 2

HHS has initiated the second phase of its HIPAA audits. Covered entities were notified July 11, 2016 and business associates received notification in the fall of 2016.

The 2016 Phase 2 HIPAA Audit Program will review policies and procedures adopted and implemented by both covered entities and their business associates to adhere to the standards of the Privacy, Security and Breach Notification Rules.

The audit program is organized by Rule and regulatory provision and addresses separately the elements of the Privacy, Security and Breach Notification.

The audit will assess the compliance with the selected requirements and will vary based on the type of covered entity or business associated selected for review.

The protocols for the audits are included in a separate Excel document.

Similar to Phase 1, the Phase 2 audit provides an opportunity to observe the mechanism for compliance, identify best practices and identify risk and vulnerabilities which may not have previously been discovered through OCR's ongoing complaint review process.

Audit Process

OCR – Verification of Customer Contact Information

Prior to sending out notification letters, OCR conducted an exercise to obtain and verify contact information for both covered entities and business associates. This information was then used to determine a list of potential auditees.

Potential Auditees

Potential auditees consist of a wide range of health care providers, health plans, health care clearinghouses and business associates.

The sampling criteria for auditees include:
a) Size of the entity
b) Affiliation with other health organizations
c) The type of entity and its relationship to individuals.
d) Public versus private
e) Geographical factors
f) Present enforcement activity with OCR.

Note: *Entities that currently have open complaint investigation or are currently involved in a compliance review will not be included in the audit.*

By selecting from a large audit pool, OCR can make an assessment of HIPAA compliance and determine its effectiveness.

OCR Communication to Covered Entities and Business Associates

OCR will be contacting organizations via email. The email will be sent from the following address OSOCRAudit@hhs.gov. It is important to confirm that the email has not been blocked by your spam filter or flagged by your organization's antivirus software.

The hhs.gov website recently reported (November 28, 2016) that a phishing email has been circulating disguised as Official OCR Audit communication. The phishing email address that is being used is **OSOCRAudit@hhs-gov.us** and directs individuals to a URL at http://www.hhs-gov.us**.**

If you do receive an email from this address, please contact HHS using the correct email OSOCRAudit@hhs.gov.

A sample of the email letter is below.

The letter is time sensitive. Upon receipt of the letter, an entity has **fourteen (14) days** to confirm their identity and email address, or provide updated primary and secondary contact information.[3]

---

[3] http://www.hhs.gov/sites/default/files/ocr-address-verification-email.pdf

DEPARTMENT OF HEALTH AND HUMAN SERVICES   **OFFICE OF THE SECRETARY**

Voice – (202) 619-0403 TDD – (202) 619-2357 FAX – (202) 619-3818
http://www.hhs.gov/ocr

Director
Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

DATE

Contact Person's Name
CE/BA 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 OSOCRAudit@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

Questionnaire

When an organization (covered entity, business associate) is contacted by OCR and their contact information has been confirmed, a questionnaire is sent.

The purpose of the questionnaire is to gather information about the size, type and operations of the potential auditees.

The data will be used along with other information to develop pools of potential auditees.

The questionnaire is made up of 4 parts:
1. Instructions
2. Contact/Entity Info
3. Questions
4. Review and Submit

Contact /Entity Info

As part of the questionnaire, review and update Contact/Entity information.

Questions

Every question requires a response.   A message will be displayed indicating the information that is still required if questionnaire is not fully completed.

The pre-screening questionnaires are listed below.

Basic Description Information about Your Organization

Question	Answer Choices
Question 1: Entity is:	• Public • Privacy
Question 2: Entity is:	• Single location only (the primary operations and any support activities are co-located) • Multi-location (the organization has multiple service delivery sites and/or separate support facilities)
Question 3: Is your organization part of, affiliated with, or otherwise owned or controlled by another organization?	• Yes • No
Question 4: If your organization is a part of, affiliated with, or otherwise owned or controlled by another organization, identify the organization and describe the relationship to your entity: (If your answer to #3 is "No", enter N/A for the relationship and organization)	• Nature of relationship • Name of other organization

Healthcare Providers

Question	Answer Choices
Question 5: Are you a HIPAA covered entity	• Yes • No
Question 6: Does your organization or another entity on your behalf, conduct health care transactions (such as submitting a claim for payment, checking patient health plan eligibility or benefit coverage, or receipt of payment or remittance advice) in electronic form?	• Yes • No
Question 7: What type of health care provider are you (hospital, urgent care, skilled nursing, etc.)?	• Fill in response
Question 8: How many patient visits in the prior fiscal year?	• Fill in response
Question 9: How many patient beds do you have (if applicable)?	• Fill in response
Question 10: What is the current number of clinicians on staff or with privileges in the facility(ies)?	• Fill in response
Question 11: Do you maintain or transmit protected health information in electronic format?	• Yes • No
Question 12: Do you use electronic medical records?	• Yes • No
Question 13: What is the total revenue for the most recent fiscal year?	• Fill in response

Health Plans

Question	Answer Choices
Question 14: Are you a Group Health Plan sponsor responding on its behalf?	• Yes • No
Question 15: What is the total number of members within your health plan(s)?	• Fill in response
Question 16: What is the average number of claims processed monthly in the most recent fiscal year?	• Fill in response
Question 17: What is the total revenue for the most recent fiscal year?	• Fill in response
Question 18: Do you utilize a third party administrator (TPA) or other entity to perform most of the health plan functions?	• No • Yes (Note: Selecting "Yes" will require you to supply the following information: "If yes, please provide the name, address, email address, phone number, an alternate contact and an appropriate contact person at the TPA or other entity (e.g., health insurance issuer or HMO):"
Question 19: If you are a group health plan sponsor, do you receive only summary data from the group health plan, health insurance issuer, or HMO?	• Yes • No • N/A

Healthcare Clearing House

Question	Answer Choices
Question 20: What is the total number of transactions processed monthly in the most recent fiscal year?	• Fill in response
Question 21: What is the current number of healthcare providers, health plans, and other entities served?	• Fill in response
Question 22: What is the total revenue for the most recent fiscal year?	• Fill in response
Question 23: Do you operate only as a business associate and do not maintain protected health information or perform covered functions as a covered entity apart from your activities as a business associate?	• Fill in response

Business Associates

Question	Answer Choices
Question 24: Please briefly describe the nature of your business associate activities (e.g., billing, third party administrator, information technology support, legal services, etc.).	• Fill in response
Question 25: Identify the type(s) of covered entity(ies) for which you provide business associate functions (choose all that apply).	• Health Care Provider • Health Plan • Heath Care Clearinghouse
Question 26: Identify whether any of the covered entity(ies) for which you provide business associate functions are Organized Health Care Arrangements (OHCA) or Affiliated Covered Entities (ACE) (choose all that apply).	• OHCA • ACE • Neither • Not sure
Question 27: Identify the approximate number of each type of covered entity for which you provide business associate functions: (please indicate a number for each option selected): NOTE: If you provide business associate functions for OHCA's or ACE's, please add the component covered entities separately into the totals below. For example, if you are a business associate to an OCHA comprised of 10 covered providers, add 10 to the covered provider total option below)	• Health Care Provider • Health Plan • Health Care Clearinghouse
Question 28: Do your business associate activities involve maintaining or transmitting protected health information in electronic form?	• Yes • No
Question 29: Do you perform business associate functions in more than one state?	• Fill in response
Question 30: What is the approximate total revenue from all of your business associate activities in the most recent fiscal year?	• Fill in response

Review and Submit

Upon completion of the questionnaire, the system will display all questions with the completed responses. Keep a copy of your responses for your records and then submit your responses. Once submitted, the questionnaire is no longer available for review.

Documenting Business Associates

As part the questionnaire process, covered entities should identify and document a list of their business associates including contact information. The contact information is required in the event that OCR selects an entity to receive a questionnaire.

Below is a link and a copy of a sample template supplied by OCR to document a list of business associates. The use of this template is optional.

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

BA Name	Type of Service Provided	POC1 Title	POC1 First Name	POC1 Last Name	POC1 Address	POC1 Address Continued	POC1 City
UNITED COUNSELING SERVICE OF BENNINGTON COUNTY, INC.		HR Director	Amy	Fella	PO BOX 588		BENNINGTON
Asociacion De Maestros De Puerto Rico		President	Aida	Diaz de Rodriguez	452 Ponce de León Ave		San Juan
Idaho Department of Health & Welfare		Privacy Officer	Heidi	Graham	PO Box 83720		Boise
NEXUS LAB, INC.		Interm Compliance Officer	Anne	Whitef	PO Box 1240		RUSSELL SPRINGS
ANTONIO ESPARZA, M.D., P.A.		Office Manager	Irene	Paramo	900 W SAM HOUSTON	SUITE1	PHARR

Refer to the appendix for a list of items requested in the template.

How the Audit Program Works

Selection of Auditees

The selection process is through random sampling of the audit pool.

Once selected, the auditees will be notified of their participation in the audit process.

Type of Audits

Desk Audits

Desk and onsite audits will be conducted for both covered entities and their business associates:
- Round 1 – Desk audits of covered entities
- Round 2 – Desk audits of business associates.

Topics Covered in the Audit

The audit will examine compliance with specific requirements of:
- Privacy
- Security or
- Breach Notification Rule

*Auditees will be notified of the subject(s) of their audit in a document request letter.

Desk Audit Completion

According to HHS, desk audit completion was targeted to be the end of December 2016.

Onsite Audits

Onsite audits will review a broader scope of requirements than desk audits.

Auditees who may have recently had a desk side audit may also be subject of an onsite audit.

Approach

Entities selected for an audit will be sent an email notification. The letter will:
- Introduce the audit team
- Explain the audit process
- Discuss OCR's expectations in more detail.
- Request initial documentation

Entities will be asked to provide documents and other data in response to a document request letter.

Auditees will submit the documents via an audit portal on OCR's website.

Auditors will review documentation and provide draft findings to the entity.

Auditees will be provided an opportunity to respond to the draft findings. These responses will be included as part of the final report. The audit report will describe how the audit was conducted, discuss any findings, and contain entity responses to the draft findings.

During the audit process, auditees should be ready for an onsite visit as requested by OCR.

Failure of an Entity to Respond to OCR's Request for Information

If an entity does not respond to request for information from OCR, including address verification pre-screening audit questionnaire and the document request, OCR will use publicly available information for its audit pool. Even if an entity does not respond to OCR, it may still be selected for an audit or subject to a compliance review.

Timeline

Desk Audits

The process is as follows:

- OCR request for information sent via email to the entity.

- Entity to submit requested information (in digital format) via the OCR secure portal within 10 days from the data requested.

- Information reviewed by the auditor who will issue draft findings to the auditee.

- Auditee has 10 days to review and provide any written updates to auditor.

- Auditor has 30 days from auditee's response to complete a final report.

A final copy of the report from OCR will be shared with the audited entity.

The same process for notification and document requests is also applicable to business associates.

A final copy of the report from OCR will be shared with the audited business associate.

Onsite Audits

The process is as follows:

- OCR notification via email.

- Auditors will schedule an entrance conference to provide details of the onsite audit process and expectations.

- On site audit from OCR can range from three (3) to five (5) days depending on the size of the entity.

- Information reviewed by the auditor who will issue draft findings to the auditee.

- Auditee has 10 days to review and provide any written updates to auditor.

- Auditor has 30 days from auditee's response to complete a final report.

- A final copy of the report from OCR will be shared with the audited entity.

Onsite audits are comprehensive covering a wider range of requirements from the HIPAA rules.

Further Investigation

If an audit indicates a compliance issue, OCR may initiate a compliance review to further investigate

After the Audit

Once the audits are conducted, OCR will review and analyze the information from both the desk and onsite audits.

This information will then be used to:

- determine types of technical assistance that should be developed
- determine types of corrective actions that would be helpful
- develop tools and guidance to assist with compliance self-evaluation
- prevent breaches.
- find risks and vulnerabilities the government is neither aware of otherwise nor likely to learn about through filed complaints[4]

---

[4] http://www.healthcareitnews.com/news/ocr-onsite-hipaa-audits-coming-2017

Appendix

Business Associates Sample Template

The following is a list of the specific information that OCR is requesting:

1. Covered entities should provide the requested information to the best of their knowledge and include the name and types of services provided by each business associate.

2. Include a secondary point of contact if that information is available.

3. Covered entities responding to the request should identify each element for each business associate.

BA Name	Type of Service Provided	POC1 Title	POC1 First Name	POC1 Last Name	POC1 Address	POC1 Address Continued	POC1 City
UNITED COUNSELING SERVICE OF BENNINGTON COUNTY, INC.		HR Director	Amy	Fela	PO BOX 588		BENNINGTON
Asociacion De Maestros De Puerto Rico		President	Aida	Diaz de Rodriguez	452 Ponce de León Ave		San Juan
Idaho Department of Health & Welfare		Privacy Officer	Heidi	Graham	PO Box 83720		Boise
NEXUS LAB, INC.		Interm Compliance Officer	Anna	Whitef	PO Box 1240		RUSSELL SPRINGS
ANTONIO ESPARZA, M.D., P.A.		Office Manager	Irene	Paramo	900 W SAM HOUSTON	SUITE1	PHARR

Question	Responsive Elements
1	Business Associate Name
2	Type of Service(s) provided
3	First Point of Contact Title
4	First Point of Contact First Name
5	First Point of Contact Last Name
6	First Point of Contact Address
7	First Point of Contact Address Continued (if needed)
8	First Point of Contact City
9	First Point of Contact State
10	First Point of Contact Zip
11	First Point of Contact Phone
12	First Point of Contact Phone Extension(if needed)
13	First Point of Contact Fax
14	First Point of Contact Email
15	Second Point of Contact Title
16	Second Point of Contact First Name
17	Second Point of Contact Last Name
18	Second Point of Contact Address
19	Second Point of Contact Address Continued (if needed)
20	Second Point of Contact City
21	Second Point of Contact State
22	Second Point of Contact Zip
23	Second Point of Contact Phone
24	Second Point of Contact Phone Extension (if needed)
25	Second Point of Contact Fax
26	Second Point of Contact Email
27	Website URL

Useful Links

Topic	Link
HIPAA Privacy Rule	https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
HIPAA Security Rule	https://www.hhs.gov/hipaa/for-professionals/security/index.html
HIPAA Breach Notification Rule	https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
Selected Protocol Elements with associated document submission requests and related Q&As - PDF	https://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf
Slides from audited entity webinar held July 13,2016- PDF	https://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf
Comprehensive question and answer listing- PDF	https://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf
Audit Protocol - *Updated April 2016*	https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
Sample Business Associates Agreement - *Published January 25, 2013*	http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
Guide to Privacy and Security of Electronic Health Information	https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
HIPAA Journal – Breach News	http://www.hipaajournal.com/category/hipaa-breach-news/
Breaches Affecting 500 or More Individuals	https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
OCR: Onsite HIPAA audits coming in 2017 Published December 7,2016	http://www.healthcareitnews.com/news/ocr-onsite-hipaa-audits-coming-2017
First Round of HIPAA Audits Exposes Providers' Weaknesses Published December 7,2016	http://www.renalandurologynews.com/hipaa-compliance/first-round-of-hipaa-audits-exposes-providers-weaknesses/article/578688/

Compliance and Enforcement Case Examples

Covered Entity
- General Hospitals
- Health Care Providers
- Health Plans/ HMO's
- Outpatient Facilities
- Pharmacies
- Private Practices

Organized by Issue
- Access
- Authorizations
- Business Associates
- Conditioning Compliance with the Privacy Rule
- Confidential Communications
- Disclosure to Avert a Serious Threat to Health or Safety
- Impermissible Uses and Disclosures
- Minimum Necessary
- Notice
- Safeguards[5]

Woman & Infants Hospital of Rhode Island (WIH), a covered entity member of Care New England Health System (CNE)[6]

Violation: Privacy and Security rules by not reviewing and updating as necessary business associate agreements.

Summary: From September 23, 2014 until August 28, 2015, WIH disclosed protected health information (PHI) and allowed its business associate, CNE, to create, receive, maintain, or transmit PHI on its behalf, without obtaining satisfactory assurances as required under HIPAA. WIH failed to renew or modify its existing written business associate agreement with CNE to include the applicable implementation specifications required by the HIPAA Privacy and Security Rules.

From September 23, 2014, until August 28, 2015, WIH impermissibly disclosed the PHI of at least 14,004 individuals to its business associate when WIH provided CNE with access to PHI without obtaining satisfactory assurances, in the form of a written business associate agreement, that CNE would appropriately safeguard the PHI.

Settlement: Monetary Amount: $400,000 and corrective action plan

---

[5] The case examples are at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/index.html

[6] http://www.hhs.gov/about/news/2016/09/23/hipaa-settlement-illustrates-importance-of-reviewing-updating-business-associate-agreements.html

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS)[7]

Violation: Business Associate's Failure to Safeguard Nursing Home Residents' PHI

Summary: Violation of the HIPAA Security rule after the theft of a mobile device that compromised the protected health information (PHI) of hundreds of nursing home residents, 412 in total.

Settlement: Monetary Amount: $650,000 and corrective action plan

---

[7] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/cathoic-health-care-services/index.html?language=es

About the Authors

Maggie Gloeckle, CIPP/US, CIPT, CIPM PMP, is Senior Privacy Officer in the financial services industry. Previously she has worked as Global Privacy Program Manager and held positions in Operations and Service Delivery Organizations. She holds a JD as well as Masters degrees in business and technology.

Professor Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. One of the world's leading experts in privacy law, Solove has taught privacy and security law since 2000, has published 10+ books and 50+ articles, including the leading textbook on privacy law and a short guidebook on the subject.

Professor Solove has spoken at hundreds of universities, federal agencies, and other organizations. He has given keynote addresses at many conferences, including one organized by the U.S. Department of Health and Human Services.

His LinkedIn blog has more than 1 million followers.

Professor Solove organizes many events per year, including the Privacy + Security Forum events, held in Washington DC in the spring and fall.

About TeachPrivacy

TeachPrivacy was founded by Professor Daniel J. Solove. He is deeply involved in the creation of all training programs because he believes that training works best when made by subject-matter experts and by people with extensive teaching experience.

TeachPrivacy has a library of nearly 100 training courses that cover a wide array of privacy and security topics including HIPAA, FERPA, PCI, phishing, social engineering, and many others.

Professor Solove's HIPAA Training

Drug Facts

Active Ingredients
HIPAA expert + engaging teacher

Effects
• Lasting memory of key points
• Highly effective prevention of incidents

Warning
So engaging that it is highly addictive.

www.teachprivacy.com