As a part of our continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the HHS Office for Civil Rights (OCR) has begun its next phase of audits of covered entities and their business associates. The 2016 Phase 2 HIPAA Audit Program will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.

Background on Phase 1 of OCR’s Privacy, Security, and Breach Notification Audit Program:

HIPAA established important national standards for the privacy and security of protected health information and the Health Information Technology for Economic and Clinical Health Act (HITECH) established breach notification requirements to provide greater transparency for individuals whose information may be at risk. HITECH requires the HHS Office for Civil Rights (OCR) to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules. In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by 115 covered entities to comply with HIPAA’s requirements. OCR also conducted an extensive evaluation of the effectiveness of the pilot program. Drawing on that experience and the results of the evaluation, OCR is implementing phase two of the program, which will audit both covered entities and business associates. As part of this program, OCR is developing enhanced protocols (sets of instructions) to be used in the next round of audits and pursuing a new strategy to test the efficacy of desk audits in evaluating the compliance efforts of the HIPAA regulated industry. Feedback regarding the protocol can be submitted to OCR at OSOCRAudit@hhs.gov.

Read more about Phase 1 of the HIPAA Audit Program.
AUDIT PHASE 2

Read the announcement: OCR Launches Phase 2 of HIPAA Audit Program.

Program Objectives:
The audit program is an important part of OCR’s overall health information privacy, security, and breach notification compliance activities. OCR uses the audit program to assess the HIPAA compliance efforts of a range of entities covered by HIPAA regulations. The audits present an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR’s ongoing complaint investigations and compliance reviews, and enable us to get out in front of problems before they result in breaches. OCR will broadly identify best practices gleaned through the audit process and will provide guidance targeted to identified compliance challenges.

When Will the Next Round of Audits Commence?
Phase Two of OCR’s HIPAA audit program is currently underway. OCR has begun to obtain and verify contact information to identify covered entities and business associates of various types and determine which are appropriate to be included in potential auditee pools. Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity’s spam filtering and virus protection are automatically enabled, we expect you to check your junk or spam email folder for emails from OCR; OSOCRAudit@hhs.gov. Click here to view a sample email letter.

Who Will Be Audited?
Every covered entity and business associate is eligible for an audit. These include covered individual and organizational providers of health services; health plans of all sizes and functions; health care clearinghouses; and a range of business associates of these entities. We expect covered entities and business associates to provide the auditors their full cooperation and support.
On What Basis Will Auditees Be Selected?

For this phase of the audit program, 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. By looking at a broad spectrum of audit candidates, OCR can better assess HIPAA compliance across the industry – factoring in size, types and operations of potential auditees. Sampling criteria for auditee selection will include size of the entity, affiliation with other healthcare organizations, the type of entity and its relationship to individuals, whether an organization is public or private, geographic factors, and present enforcement activity with OCR. OCR will not audit entities with an open complaint investigation or that are currently undergoing a compliance review.

How Will the Selection Process Work?

Once entity contact information is obtained, a questionnaire designed to gather data about the size, type, and operations of potential auditees will be sent to covered entities and business associates. This data will be used with other information to develop pools of potential auditees for the purpose of making audit subject selections. Click here to view the audit pre-screening questionnaire.

OCR will be asking covered entity auditees to identify their business associates. We encourage covered entities to prepare a list of each business associate with contact information so that they are able to respond to this request.

OCR will choose auditees through random sampling of the audit pool. Selected auditees will then be notified of their participation. Click here to view a sample template entities may use to develop their list of business associates. Use of this template is optional.

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 Will the Audit Program Work?

OCR plans to conduct desk and onsite audits for both covered entities and their business associates. The first set of audits will be desk audits of covered entities followed by a second round of desk audits of business associates. These audits will examine compliance with specific requirements of the Privacy, Security, or Breach Notification Rules and auditees will be notified of the subject(s) of their audit in a document request letter. All desk audits in this phase will be completed by the end of December 2016.

The third set of audits will be onsite and will examine a broader scope of requirements from the HIPAA Rules than desk audits. Some desk auditees may be subject to a subsequent onsite audit.

The audit process will employ common audit techniques. Entities selected for an audit will be sent an email notification of their selection and will be asked to provide documents and other data in response to a document request letter. Audited entities will submit documents on-line via a new secure audit portal on OCR’s website. There will be fewer in person visits during these Phase Two audits than in Phase One, but auditees should be prepared for a site visit when OCR deems it appropriate. Auditors will review documentation and then develop and share draft findings with the entity. Auditees will have the opportunity to respond to these draft findings; their written responses will be included in the final audit report. Audit reports generally describe how the audit was conducted, discuss any findings, and contain entity responses to the draft findings.
What if an Entity Doesn’t Respond to OCR’s Requests for Information?

If an entity does not respond to requests for information from OCR, including address verification, the pre-screening audit questionnaire and the document request of those selected entities, 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.

What is the General Timeline for an Audit?

In the coming months, OCR will notify the selected covered entities in writing through email about their selection for a desk audit. The OCR notification letter will introduce the audit team, explain the audit process and discuss OCR’s expectations in more detail. In addition, the letter will include initial requests for documentation. OCR expects covered entities that are the subject of an audit to submit requested information via OCR’s secure portal within 10 business days of the date on the information request. All documents are to be in digital form and submitted electronically via the secure online portal.

After these documents are received, the auditor will review the information submitted and provide the auditee with draft findings. Auditees will have 10 business days to review and return written comments, if any, to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee’s response. OCR will share a copy of the final report with the audited entity.

While conducting desk audits of covered entities, OCR will replicate the notification and document request process for initiating desk audits of selected business associates. OCR will share a copy of the final report with the audited business associate.

Similarly, entities will be notified via email of their selection for an onsite audit. The auditors will schedule an entrance conference and provide more information about the onsite audit process and expectations for the audit. Each onsite audit will be conducted over three to five days onsite, depending on the size of the entity. Onsite audits will be more comprehensive than desk audits and cover a wider range of requirements from the HIPAA Rules. Like the desk audit, entities will have 10 business days to review the draft findings and provide written comments to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee’s response. OCR will share a copy of the final report with the audited entity.

What Happens After an Audit?

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. Generally, OCR will use the audit reports to determine what types of technical assistance should be developed and what types of corrective action would be most helpful. Through the information gleaned from the audits, OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches.

Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to further investigate. OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity. However, under the Freedom of Information Act (FOIA), OCR may be required to release audit notification letters and other information about these audits upon request by the public. In the event OCR receives such a request, we will abide by the FOIA regulations.
How Will Consumers Be Affected?

The audit program is an important tool to help assure compliance with HIPAA protections, for the benefit of individuals. For example, the audit program may uncover promising practices, or reasons health information breaches are occurring and will help OCR create tools for covered entities and business associates to better protect individually identifiable health information. Concerns about compliance identified and corrected through an audit will serve to improve the privacy and security of health records. The technical assistance and promising practices that OCR generates will also assist covered entities and business associates in improving their efforts to keep health records safe and secure. During the audit process, OCR will continue to accept complaints from individuals and to launch compliance reviews where warranted; covered entities and business associates’ compliance obligations remain in full effect.

Will Audits Differ Depending on the Size and Type of Participants?

The audit protocols are designed to work with a broad range of covered entities and business associates, but their application may vary depending on the size and complexity of the entity being audited.

Will Auditors Look at State-Specific Privacy and Security Rules in Addition to HIPAA’s Privacy, Security, and Breach Notification Rules?

No, the scope of the audit program does not extend beyond the Privacy, Security, and Breach Notification Rules.

Who is Responsible for Paying the On-Site Auditors?

The Department of Health and Human Services is responsible for the on-site auditors. Neither covered entities nor their business associates are responsible for the costs of the audit program.