COMPLIANCE BULLETIN

HHS Launches HIPAA Audit Program

HIGHLIGHTS

- HHS has announced the start of the second phase of its HIPAA audit program.
- Both covered entities and business associates may be selected for a HIPAA audit.
- If a HIPAA audit reveals a serious compliance issue, HHS may initiate a compliance review to investigate further.

DEADLINES

- Entities selected for an audit will be asked to provide information regarding HIPAA compliance.
- Audited entities will have **10 business days** to submit the requested information.
- After OCR develops its draft findings, audited entities will have **10 business days** to review the findings and respond to OCR.

Provided By:
BenefitsContinuum

OVERVIEW

The Department of Health and Human Services (HHS) announced that it has launched the second phase of its HIPAA audit program, which focuses on compliance with HIPAA's Privacy, Security and Breach Notification Rules.

This second phase of the HIPAA audit program covers both covered entities and business associates. HHS' Office for Civil Rights (OCR) has already started sending emails to covered entities and business associates to verify their contact information. Next, OCR will send a pre-audit questionnaire to gather data about potential auditees. OCR will use this data to select covered entities and business associates for audits.

According to OCR, these HIPAA audits are primarily a compliance improvement activity. However, if an audit reveals a serious compliance issue, OCR may initiate a compliance review to investigate.

ACTION STEPS

To prepare for a possible HIPAA audit, covered entities and business associates should review their compliance with HIPAA's Privacy, Security and Breach Notification Rules.

benefitsContinuum
Think ahead…Stay ahead

OCR has stated that it will post an updated audit protocol on its website closer to conducting the 2016 audits. Once it is available, this audit protocol can be used as a guide for internal self-audits of HIPAA compliance.

Also, because communications from OCR will be sent via email and may be incorrectly classified as spam, OCR expects covered entities and business associates to check their junk or spam email folders for emails from OCR (OSOCRAudit@hhs.gov). An entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.

BACKGROUND

HIPAA established national standards for the privacy and security of protected health information (PHI) and the Health Information Technology for Economic and Clinical Health (HITECH) Act established breach notification requirements to provide greater transparency for individuals whose information may be at risk.

OCR is responsible for enforcing the HIPAA 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. Through those audits, OCR developed an audit protocol and identified some overall findings and observations.

The HITECH Act requires OCR to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security and Breach Notification Rules.

NEW AUDIT PROGRAM

Drawing on its experience from the pilot audit program, OCR is implementing the second phase of its HIPAA audit program, which covers 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 effectiveness of desk audits in evaluating HIPAA compliance.

OCR will post updated audit protocols on its website closer to conducting the 2016 audits. The audit protocol will be updated to reflect the HIPAA Omnibus Rulemaking and can be used as a tool by organizations to conduct their own internal self-audits as part of their HIPAA compliance activities.

When Will the HIPAA Audits Begin?

The second phase 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. A sample email letter from OCR is available here.

Who Will Be Audited?

Every covered entity and business associate is eligible for an audit. According to OCR, it 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.

The sampling criteria for auditee selection includes the 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 compliance investigation or that are currently undergoing a compliance review.

How Does the Pre-audit Screening Process Work?

OCR will first contact a covered entity or business associate to verify contact information. Once this information is verified, OCR will send the covered entity or business associate a questionnaire designed to gather data about its size, type and operations. As a part of the pre-audit screening questionnaire, OCR is asking that entities identify their business associates.

OCR will conduct a **random sample** of entities in the audit pool. The covered entities and business associates that are selected for an audit will then be notified by OCR. 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 Does the Audit Program Work?

OCR plans to conduct desk and on-site audits for both covered entities and their business associates.

1	The first round of audits will be **desk audits of covered entities**	All desk audits in this phase will be completed by December 2016
2	The second round of audits will be **desk audits of business associates**	
3	The third round of audits will be **on-site audits**	On-site audits will examine a broader scope of requirements from the HIPAA Rules than desk audits. Some desk auditees may be subject to a subsequent on-site audit.

Desk Audits

According to OCR, the process for **desk audits** works as follows:

- ✓ 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 online via a **new secure audit portal** on OCR's website. OCR expects audited entities to submit the requested information within **10 business days** of the date on the information request. There will be fewer in-person visits during this second phase of audits, 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 audited entity.
- Audited entities will have **10 business days** to review and respond to these draft findings. 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.

On-site Audits

Covered entities and business associates will also be notified via email of their selection for an **on-site audit**. The auditors will schedule an entrance conference and provide more information about the on-site audit process and expectations for the audit. Each on-site audit will be conducted over **three to five days on site**, depending on the size of the entity.

On-site audits will be 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 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?

According to OCR, audits are primarily a **compliance improvement activity** that 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.

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

OCR will not post a listing of audited entities or the findings of an individual audit that 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.

Source: Department of Health and Human Services