FYI®
For Your Information®

Volume 39 | Issue 45 | April 8, 2016

Office for Civil Rights HIPAA Audits Underway

The HHS' Office for Civil Rights, tasked with completing HIPAA compliance audits, announced that it has begun Phase 2 of the HIPAA audit program. All covered entities (including group health plans) and business associates have the potential of being selected for a desk or onsite audit. Entities should be on the lookout for emails from OCR soliciting contact information and, in the coming months, notification of selection for audit.

Background

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) require covered entities (health care providers, health plans and health care clearing houses) to comply with privacy, security, and breach notification rules with respect to individuals' protected health information (PHI). (See our March 8, 2013 *For Your Information*.) HITECH also requires the Department of Health and Human Services' Office for Civil Rights (OCR) to conduct audits of covered entities and their business associates to ensure compliance with the HIPAA rules. OCR conducted a pilot program in 2011 and 2012 where it audited covered entities for HIPAA compliance. Now, based on the results of the pilot program, OCR is beginning the next phase of the audit program.

Phase 2 Already In Progress

Phase 2 of the audit program, under which OCR will review the HIPAA policies and procedures of covered entities and their business associates, has already begun. OCR is creating a pool of potential auditees by sending emails to covered entities and business associates to request and verify entity contact information.

> **Comment.** Because OCR is communicating by email and the email may be incorrectly classified as spam, covered entities and business associates should regularly check spam and junk folders for communication from OCR.

Check your spam folder!

OCR's emails may be incorrectly classified as spam.

OCR's email address is: OSOCRAudit@hhs.gov.

Who Will Be Audited?

All covered entities and business associates may be audited. OCR is identifying pools of covered entities and business associates that represent a wide range of health care providers, health plans and health care clearinghouses for audit. To that end, it will consider size of the entity, affiliation with other health care 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 compliance review.)

After OCR receives entity contact information (as noted above), it will send a pre-audit questionnaire to gather data about the size, type and operations of the entities. The questionnaire will also ask covered entities to identify their business associates. This information will be used to create an audit subject pool. OCR will randomly select entities from the pool for participation.

> **Comment.** Failure to reply to OCR's requests for information will not shield an entity from audit. Instead, OCR will use publicly available information about the entity to add to the subject pool.

What Can I Expect From the Audit?

While most will be desk audits, OCR will conduct some onsite audits. OCR intends to start with desk audits of covered entities followed by desk audits of business associates. A third set of audits will be onsite and will examine a broader scope of HIPAA requirements than desk audits.

Common Business Associates

- Insurers and HMOs covered by ASO agreements to provide claims processing and medical management decisions
- Third-party vendors (e.g., COBRA, disease management, utilization review)
- Lawyers
- Consultants and actuaries
- Pharmacy benefit managers
- Accountants
- Patient safety organizations
- Data storage companies (digital or hard copy); entities that offer personal health records to individuals on behalf of covered entities; data aggregators
- Health information organizations (HIOs), e-prescribing gateways, and subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate

OCR will notify entities selected for desk audits by email. The email will explain the subject of the audit and will request documents and other information. Selected entities will have ten business days to submit the requested information online through a secure audit portal on OCR's website. OCR will also notify entities selected for onsite audits by email. The auditors will schedule a three- to five-day onsite visit. Entities selected for onsite visits can expect a more comprehensive audit than the desk audits.

In both cases, the auditor will review the information and share draft findings with the entity. The entity will have ten business days to review and comment on the draft findings. Within 30 business days of receiving the entity's comments, the auditor will prepare a final audit report describing how the audit was conducted, any findings, and the entity's responses to the draft findings.

What's the Purpose of the Audit?

The audits are intended to improve compliance. OCR will use information from the audit reports to determine what technical assistance and types of corrective action would be most beneficial. It will also create tools and guidance to help with self-evaluation of compliance and prevent breaches of protected health information.

If an audit reveals serious compliance issues, OCR may initiate a compliance review for further investigation.

What Should I Do Now?

The turnaround time for providing documents and other information, if selected for an audit, is very short. Entities should prepare now for the possibility of an audit. Important tasks include:

- Inventory all HIPAA documentation: policies and procedures, privacy notice, business associate agreements and complete list of business associates with contact information, training materials, security risk assessments, breach notifications
- Remediate any deficiencies in HIPAA documentation
- Regularly check spam and junk email folders for communication from OCR
- Watch for an updated audit protocol on OCR's website

In Closing

With the HIPAA audit process already begun, entities should promptly confirm that HIPAA compliance is in order. Because OCR will give very little time to provide documentation, entities should take action now to ensure a smooth process if selected.

Authors
Kimberley Mitchell, JD
Amy Dunn, JD, MHA

Produced by the Knowledge Resource Center of Xerox HR Consulting
The Knowledge Resource Center is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your account executive or email fyi@xerox.com.