TRUCKER ✦ HUSS

Be Prepared for Phase Two of the HIPAA Audit Program

ELIZABETH LOH

Introduction

On March 21, 2016, the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") launched Phase Two of its Health Insurance Portability and Accountability Act ("HIPAA") Audit Program. In this phase of the HIPAA Audit Program, the OCR intends to audit a wide variety of covered entities (including health plans of all sizes) and business associates to determine whether these entities are meeting their HIPAA Privacy, Security, and Breach Notification obligations. In light of the launch of Phase Two of the Audit Program, covered entities and their business associates should take action to prepare for possible audit.

General Background

The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") requires the OCR to proactively conduct periodic audits of HIPAA covered entities (*i.e.*, health plans, health care providers, and health care clearing houses), and business associates to assess compliance with the HIPAA Privacy, Security, and Breach Notification rules. A covered entity is selected at random for audit, thus selection is not necessarily related to a particular incident or HIPAA complaint. OCR plans on using its Audit Program to identify best practices and discover potential HIPAA risks and vulnerabilities.

In Phase One of the HIPAA Audit Program, OCR implemented a "pilot audit program" where it audited 115 covered entities (47 of which were health plans). After analyzing the results of this "pilot audit program," OCR submitted a report to Congress on HIPAA compliance. This report is illuminating because it spells out the areas where covered entities "fell short" in their HIPAA compliance efforts. These areas included:

- Providing individuals with the Notice of Privacy Practices;
- Addressing the rights of individuals to access their protected health information;
- Obtaining HIPAA authorizations;
- Conducting HIPAA Security Risk Assessments; and
- Implementing the appropriate procedures for securing electronic protected health information ("ePHI") that is stored and/or transported on portable electronic devices.

OCR is using the information it gathered during the pilot audit program to implement Phase Two of the HIPAA Audit Program.

Phase Two of the HIPAA Audit Program Has Begun

OCR has announced that Phase Two of the HIPAA audit program is currently underway.

Who Is Subject to Audit?

According to the OCR announcement, "every covered entity and business associate is eligible for audit." OCR intends to create an audit pool that represents a wide range of health care providers, health plans, health care clearing houses and business associates. OCR has further clarified that it is looking to audit health plans of all sizes and functions.

How Will a Covered Entity Know if It Has Been Selected for Audit?

OCR has begun its audit selection process by sending out targeted emails to covered entities. These OCR emails ask the covered entity to verify that the contact information OCR has on record (*e.g.*, primary contact information, email address) is accurate.

Once OCR has obtained the covered entity's contact information, it will send the covered entity a pre-screening questionnaire. This pre-screening questionnaire is designed to gather information regarding the covered entity's type, size, and operations. For example, health plans must answer questions regarding the "average number of claims processed monthly," and the "number of members covered by the health plan." As part of this pre-screening process, OCR also will ask the covered entity to provide a list of its business associates. To assist covered entities with this process, OCR has created a template that a covered entity may use when developing its list of business associates. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html

Once the pre-screening process is complete, OCR intends to build a diverse audit pool based on the information it has gathered from the pre-screening questionnaires. OCR will randomly select covered entities (and business associates) from this audit pool.

Note: OCR has stated that it will use publically available information for covered entities that do not respond to OCR's contact information or pre-audit questionnaire, thus a non-responsive covered entity may still be selected for audit or subject to a compliance review.

How Will the HIPAA Audit Program Work?

OCR plans on conducting both desk audits and on-site audits. OCR will first conduct desk audits of covered entities, followed by a round of desk audits of business associates. The third round of audits will consist of on-site audits.

OCR explains the desk audit process as follows:

1. In the coming months, OCR will notify a covered entity via email if it has been selected for a desk audit. The OCR notification letter will introduce the audit team, explain the audit process, and include a document request.

2. The covered entity has ten business days to supply the information requested by OCR. The covered entity will submit the requested documents on-line via OCR's "secure on-line portal."

3. Upon receiving the covered entity's documents, the OCR auditor will review the information submitted and provide the covered entity with its draft findings. The covered entity will have ten business days to review the draft findings and provide written comments to the OCR auditor.

4. The OCR auditor will complete a final audit report for the covered entity within 30 business days after the covered entity's response. OCR will share a copy of the final audit report with the covered entity.

After conducting the desk audits, OCR will conduct on-site audits. OCR anticipates that the on-site audits will be more comprehensive than the desk audits. Each on-site audit will be conducted over a period of three to five days. It's important to note that a covered entity that is subject to a desk audit may also be subject to a subsequent on-site audit by OCR.

What Happens After the Audit?

These audits are primarily a compliance improvement activity. OCR will use the audit results to determine what types of technical assistance it should develop to assist covered entities (and business associates) with their HIPAA compliance efforts. However, if an audit report shows that a covered entity (or business associate) has serious HIPAA compliance issues, OCR may initiate a compliance review and investigate further.

How Can I Prepare for an Audit?

Given OCR's launch of Phase Two of the HIPAA Audit Program, employers/plan sponsors should proactively take steps to prepare for potential audit. Examples of steps to take include:

- Take inventory of your group health plans to determine which plans are subject to HIPAA compliance (*e.g.*, Health Flexible Spending Accounts, self-funded medical, dental, vision plans, etc.).
- Evaluate whether you have entered into HIPAA compliant business associate agreements with your group health plan vendors.
- Prepare a list of your business associates (with each business associate's contact information) so that you are prepared to respond to potential OCR requests.
- Review your Notice of Privacy Practices to verify that it is HIPAA compliant, and timely distribute this Notice to group health plan participants as required under the HIPAA rules.
- Verify that you have the appropriate HIPAA policies and procedures in place (including documentation).
- Regularly conduct HIPAA training for your workforce.
- Conduct HIPAA security risk assessments and document these assessments.

- Develop procedures for protecting ePHI that is stored or transported by portable electronic media (*e.g.*, laptops, USB storage devices, etc.).
- Look for emails from OCR requesting confirmation of your contact information. OCR recommends checking your junk or spam email folders in case OCR emails are incorrectly classified as spam.
- Review the Audit Protocol published by OCR. The Audit Protocol includes compliance questions that auditors may ask. This Audit Protocol was recently updated for Phase Two of the Audit Program and the HIPAA Omnibus Rules. A link to the updated Audit Protocol is included here http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/

If you have any questions regarding this article, please contact the author.

APRIL 2016