FRENKELBENEFITS
Employee Benefits Broker & Consultant
COMPLIANCE UPDATE

OCR Phase 2 HIPAA Audits Underway

Issue Date: August 2016

Introduction

The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) has begun Phase 2 of its HIPAA Audit Program. The scope of this national audit includes covered entities and business associates of various industries and sizes, and all covered entities and business associates are eligible to be audited. Employers offering plans subject to HIPAA, along with employers acting as business associates for covered entities, should review current HIPAA compliance efforts to make sure all requirements are addressed; watch for communications from OCR; and respond to any inquiries from OCR within the required time frames.

Background

The Audit Program was launched following the passage of HITECH, which required HHS to perform periodic audits of covered entities and business associates to ensure compliance with the Privacy and Security Rules, as well as with HITECH's breach notification standards. Phase 1 of the audit program was completed in 2011 and 2012, and consisted of a "pilot program" that focused on 115 covered entities. OCR reviewed the privacy and security compliance documentation of these covered entities, conducted site visits, and provided draft and final audit reports. Since then, OCR has been evaluating its audit protocol in preparation for Phase 2 in order to make improvements and ensure that the next round is effective.

In general, OCR has indicated that the purpose of the audit is to assess overall compliance with the HIPAA Privacy and Security Rules, as well as with the breach notification requirements under the Health Information Technology for Economic and Clinical Health (HTECH) Act of 2009. This includes identifying industry best practices, along with risks and vulnerabilities not detected through current enforcement activities. It will use the results of these audits to develop tools and guidance to assist the industry with compliance self-evaluation and prevention of breaches of unsecured protected health information (PHI).

Summary

Audit Structure and Timing

Phase 2 of the Audit Program consists of three distinct stages: Stage 1 consists of desk audits of covered entities, while Stage 2 will consist of desk audits of business associates. These desk audits will focus specifically on the auditee's compliance with the Privacy, Security, and Breach Notification requirements. During Stage 3, OCR will conduct onsite audits lasting 3-5 days, during which it will review a more comprehensive set of HIPAA requirements. Both desk and onsite audits will culminate in a draft report from OCR, to which the auditee has ten (10) business days to issue a written response. OCR will issue a final report outlining its findings within thirty (30) business days of receipt of the auditee's response to the draft report.

Desk audits of covered entities are currently underway, with desk audits of business associates scheduled to begin in late September. OCR has indicated that it expects to complete its desk audits by the end of December 2016, and that onsite audits will begin in early 2017.

Selection and Notification Process

Earlier this year, OCR reached out to covered entities of various sizes and from various industries to gather contact information, which it then used to develop its potential audit pool. Once it obtained contact information, it sent a pre-audit questionnaire to potential auditees. If an entity did not respond to a request for contact information or to the pre-audit questionnaire, OCR gathered the information using publicly available information. From this larger pool, OCR selected its final audit pool of covered entities using a randomized selection algorithm.

OCR has indicated that its final selection of business associates will draw primarily from the lists provided by covered entities as part of the document request described below. Business associates will be subject to the same requirements for providing responses to the audit questionnaires.

While the onsite audits will generally be conducted on a different pool of auditees than the desk audits, OCR has indicated that some entities that receive desk audits may also be subject to a subsequent onsite audit. The most recent numbers provided by OCR indicate that it will audit approximately 200-250 covered entities and business associates. Of this total, over 200 will be desk audits, with a smaller number of comprehensive onsite audits.

OCR has indicated that it will send its communications via email from OSOCRAudit@hhs.gov, which may be routed to an entity's spam folder. Entities are responsible for checking spam folders to ensure communications are not missed.

Scope of Audit

Whereas onsite audits will involve a more comprehensive review of HIPAA compliance controls, desk audits for covered entities are focusing on seven (7) controls drawn from the Security Rule, the Privacy Rule, and the Breach Notification Rule:

1. Privacy Rule Controls:
    a. Notice of Privacy Practices and Content Requirements
    b. Provision of Notice – Electronic Notice
    c. Right to Access [protected health information]
2. Breach Notification Rule Controls:
    a. Timeliness of Breach Notification
    b. Content of Breach Notification
3. Security Rule Controls:
    a. Security Management Process – Risk Analysis
    b. Security Management Process – Risk Management

Auditees will be audited either on Security Rule controls compliance or on Privacy Rule/Breach Notification Rule controls compliance (but not both).

OCR is issuing two (2) separate document requests via email: one for policies and procedures (and related documentation), and another for a list of business associates. Auditees must submit the requested policies and procedures via OCR's online portal (a link will be included in the email request). Entities should submit Business Associate lists via email. If an entity does not have the requested documentation, it must submit an explanation for the deficiency in its response.

It is expected that the desk audits for business associates will follow a protocol similar to the one being used for covered entities, although different controls may be included.

Summary

It is important for all entities responsible for compliance with HIPAA, including employers sponsoring health plans subject to HIPAA and employers who are business associates, to prepare for a potential audit. The audit protocol highlights areas that all covered entities and business associates should pay attention to in order to avoid potential breaches or other incidents that may invite enforcement action. Entities should review current compliance efforts, including ensuring that they, to the extent applicable: 1) have policies and procedures in place, including breach notification procedures; 2) have a current Notice of Privacy Practices; 3) have conducted a risk analysis and inventory of PHI; 4) have appropriate Business Associate Agreements in place; 5) have designated Privacy and Security Officials; and 6) have conducted privacy and security training for relevant employees.

Additional information about Phase 2 Audits may be found on the OCR's website using the link below. Information includes sample email notification letters, a copy of the audit protocol, sample templates for identifying business associates, Q&As, and a copy of the pre-screening questionnaire. Slides from a July presentation on the Phase II audit process are also available.

OCR's Audit Program website may be found here:
http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#program

Please be aware that this does not represent legal or tax advice and is only Frenkel's interpretation of the laws, regulations and statutes. It is highly recommended that you seek the advice of your legal and tax professional as to the applicability of this information to your particular situation.