April 7, 2016

HIPAA Compliance and the Phase 2 Audit Program

Data theft with respect to medical information is on the rise, and consequently compliance with the Health Insurance Portability and Accountability Act (HIPAA) is more important than ever. In an effort to combat such theft and protect the confidentiality of individuals' health information, the HIPAA rules require that covered entities implement measures to keep certain health information protected. Group health plans as covered entities are required to comply with these rules although many health plan sponsors have historically been lax about HIPAA compliance. The government is taking a more aggressive approach toward HIPAA compliance and the Department of Health and Human Services' Office for Civil Rights (OCR) has recently embarked on the next phase of a HIPAA audit program. Under this program, all covered entities, including group health plans may be subject to audit and employers that sponsor group health plans, should be aware that they might receive communications and pre-HIPAA audit questionnaires from the OCR regarding compliance with HIPAA. In preparation for coming OCR audits described herein, employer group health plans should review their policies and procedures for compliance with the HIPAA rules and determine whether these policies and procedures need to be revised or updated to reflect current practices.

OCR HIPAA Audit Program

In its original attempt to verify compliance with the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule, OCR piloted privacy and security audits of covered entities in 2011 and 2012 (the "Phase 1 Audits"). In general, HIPAA covered entities include healthcare clearinghouses, healthcare providers (that engage in certain electronic transactions such as billing for services), and health plans (including health insurers and self-funded employer-group health plans). OCR is now beginning its "Phase 2" Audit Program to 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. Phase 2 Audits will consist of more than 200 desk and onsite audits of both covered entities and business associates. The Phase 1 program conducted in 2011 and 2012 targeted only covered entities and involved just 115 audits.

Phase 2 Audits

The Phase 2 Audits will primarily be desk audits, although some on-site audits will be conducted. According to an OCR press release, Phase 2 will include "a broad spectrum of audit candidates" that OCR will randomly select from pools representing "a wide range of healthcare providers, health plans, healthcare clearinghouses and business associates." Audits are an important compliance tool for OCR, supplementing OCR's other enforcement tools, such as complaint

investigations and compliance reviews. These tools enable OCR to identify best practices and proactively uncover and address risks and vulnerabilities to protected health information (PHI). The process for the Phase 2 Audits is as follows:

- *Request for Contact Information:* OCR has already begun sending out email communications requesting that covered entities and business associates confirm or provide their contact information to OCR. The individual identified to OCR as the primary contact at covered entities and business associates should be on the lookout for email communications from OCR, including checking their junk or spam email folders for emails from OCR. If an entity's spam filtering and virus protection are automatically enabled, OCR expects entities to check their junk or spam email folder for emails from OCR. When a covered entity or business associate does not respond to a communication from OCR, OCR will use publically available information to create its audit pool, and the entity may nevertheless be selected for an audit or subject to a compliance review.
- *Pre-Audit Questionnaire:* Once contact information is verified, OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees. This data will be used with other information to identify pools of covered entities and business associates that represent a wide range of healthcare providers, health plans, healthcare clearinghouses, and business associates. Sampling criteria for audit 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 current enforcement activity with OCR. At this stage, covered entities will also be asked to identify their business associates (with contact information).
- *Desk Audit:* Entities selected for audit will be subject to a desk audit (an examination of documents and records) and, if necessary, an on-site audit. OCR will review HIPAA policies and procedures adopted and utilized by covered entities and their business associates. Desk audits of covered entities and business associates will examine compliance with specific requirements of the HIPAA rules. Entities selected for a desk audit will be notified by email of their selection and will be asked to provide documents and other data. Audited entities will be required to submit documents online via a new secure audit portal on OCR's website. Desk audits will be completed by the end of December 2016.
- *On-Site Audit:* After the desk audits, OCR will conduct onsite audits to examine "a broader scope of requirements from the HIPAA Rules than desk audits." Entities will be notified of their selection for an on-site audit via email. Desk auditees may be subject to a subsequent onsite audit. 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.
- *Follow-up:* At the conclusion of desk audits and onsite audits, OCR will provide the auditee with a report of their findings. While Phase 2 audits are not intended "to be a punitive mechanism," in the event that a serious compliance issue is identified in an audit report, OCR may begin a HIPAA compliance review. After the audit process, OCR will review and analyze the information from the final reports to determine what types of technical assistance should be developed and what types of corrective action would be most helpful, and then work to develop tools and guidance to assist the HIPAA-regulated industry in compliance self-evaluation and in preventing breaches.

Visit the OCR website to learn more about the Phase 2 Audit program.

Preparation for Audit

OCR intends to evaluate the results and procedures used in its Phase 2 Audits to develop a permanent audit program. Employer group health plans should review their policies and procedures for compliance with the HIPAA rules and determine whether these policies and procedures need to be revised or updated to reflect current practices. It is important to note that HIPAA compliance obligations with respect to group health plans may vary between plan sponsors and are influenced by a variety of factors including a health plan's funding arrangement, the plan's access to individually identifiable health information and operational and/or administrative practices. For example, self-insured plan sponsors with access to individuals' health information may have significantly greater HIPAA compliance obligations than a fully insured health plan sponsor with no access to individuals' health information. In preparation for the Phase 2 Audit process, covered entities may need to:

- Carefully review their privacy and security policies, compile evidence that the policies have been implemented and enforced, and be able to demonstrate that they reviewed and updated policies in light of changes in law, operations and information technology standards;
- Conduct and/or update Security Rule risk assessments (as lack of proper risk assessment was a repeated observation during the Phase 1 Audits);
- Review covered entity and business associate relationships to ensure compliance with HIPAA;
- Review training programs and ensure workplace training has occurred and is up-to-date;
- Review compliance with an enhanced focus on certain high-risk areas including: (1) patient's rights to access their personal health information; (2) authorizations; (3) minimum necessary use and disclosure; (4) encryption of electronic transmission, mobile devices, and devices containing protected health information (USB drives, etc.); (5) logging; (6) access controls; (7) notice of privacy practices; and (8) breach notification (including the content and timeliness of a breach notification).

For additional information/assistance, see the OCR website dedicated to HIPAA compliance for a summary of the many obligations that may fall under the HIPAA privacy and security rules. Contact your Conner Strong & Buckelew account representative toll free at 1-877-861-3220 should you have any questions. For a complete list of Legislative Updates issued by Conner Strong & Buckelew, visit our online Resource Center.