PUBLICATION

Are You Ready? New Round of HIPAA Audits Are Underway

Authors: Alisa L. Chestler
March 22, 2016

On March 21, 2016, the Office for Civil Rights (OCR) formally announced the start of its 2016 Phase 2 Health Insurance Portability and Accountably Act (HIPAA) Audit Program. Unlike Phase 1, in which OCR's 2012 pilot program audited covered entities only for HIPAA privacy and security compliance, the Phase 2 Audit Program is more expansive in scope, applying to covered entities and business associates. OCR is using the Phase 2 Audit Program to assess the HIPAA compliance efforts of a range of HIPAA-regulated entities and has stated that the audits "present an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews." Though OCR has stated that the Phase 2 Audit Program is primarily intended to be a "compliance improvement activity," make no mistake; if serious compliance issues are discovered, OCR may initiate a compliance review to investigate further. While OCR promises to provide more details in the future, here is what we know now about OCR's Phase 2 Audit Program:

- **OCR's Pre-Audit Process Will Be Initiated Via Email**. OCR has begun to reach out to potential auditees via email to verify contact information. This process is expected to identify covered entities and business associates of various types and will be used to determine which are appropriate to include in the potential auditee pools. It is important to note that emails may be incorrectly classified as spam, and OCR has expressly stated that it expects covered entities and business associates to check junk and spam email folders for emails from OCR originating from OSOCRAudit@hhs.gov.
- **Covered Entities and Business Associates of All Shapes and Sizes Will Be Audited**. Every covered entity and business associate is eligible to be audited. This means that health care providers, health plans and health care clearinghouses, as well as a range of their respective large and small business associates, could be selected.
- **Auditee Selection Will Be Based on Various Criteria**. OCR will look at a broad range of audit candidates so it can better assess compliance across the industry. To accomplish this goal, OCR will base its selection on size of the entity, affiliation with other health care organizations, type of entity and its relationship to individuals, whether the organization is public or private, geographic factors and present enforcement activities. OCR will not include any entity that has an open complaint investigation or that is currently undergoing a compliance review.
- **Selection Process Will Be Based on Pre-Audit Screening Questionnaire**. After receipt of contact information, OCR will send a pre-audit screening questionnaire to gather data about the size, type and operations of potential auditees. OCR will ask entities to identify their business associates in this questionnaire. Privacy officials should be prepared to respond quickly to such requests as there will be tight timelines in which responses are due. Based on the responses to these questionnaires, OCR will create "audit pools," which are presumably comprised of covered entities and their business associates. From the audit pools, OCR will select a random sample of entities for audit and the selected auditees will be notified of their participation in a document request letter that is sent via email.
- **Desk and On-Site Audits Will Be Conducted**. OCR intends to split the audits into three sets. The first two sets will be desk audits. The first set will be for covered entities and the second for business associates. The desk audits will examine policies and procedures for compliance with specific requirements of the HIPAA Privacy, Security and Breach Notification Rules. The third set will be

onsite audits, which will examine a broader scope of requirements than the desk audits. Some desk auditees may be subject to onsite audits. OCR anticipates concluding both sets of desk audits by the end of 2016. No schedule has been provided for when the desk or onsite audits will commence.

- **An Audit Portal Will Be Used to Submit Documentation for Desk Audit**. OCR will require the auditees to submit requested documentation and other data "online via a new audit portal on OCR's website." Requested documentation must be submitted via the online portal within 10 business days of OCR's request, which is a very tight timeframe. Failure to submit a timely response presumably will result in a negative finding.
- **On-Site Auditees Will Be Notified Via Email**. OCR will notify entities of their selection for the on-site audit via email. An entrance conference will be scheduled and the onsite audit will be conducted over a three-to-five day timeframe depending on the size of the entity. As previously noted, on-site audits will be more expansive than desk audits.
- **Audit Protocols Will Be Used**. OCR will use audit protocols that are designed to apply to a broad range of covered entities and business associates. The application of the audit protocols will vary based on the size and complexity of the entity audited. OCR intends to publish the protocols on its website closer to the time of conducting the audits in 2016.
- **Audit Findings Will Be Provided to Auditees with Rebuttal Opportunity**. OCR auditors will prepare draft findings based on the documentation submitted in the desk or onsite audit review. Auditees will have 10 business days to review and return written comments, if any. Final audit reports will then be provided to the entity within 30 business days after the auditee's response. Depending on the results of the audit, OCR may provide technical assistance to the auditee and potentially require corrective actions. If serious compliance issues are revealed through the audit, OCR may initiate a compliance review.
- **Auditees and Audit Findings Will Not Be Posted**. OCR has stated that neither the list of auditees nor the audit findings will be posted. However, audit notification letters and other audit information may be made public in accordance with the Freedom of Information Act (FOIA) requests.
- **Failure to Respond to OCR Requests Will Not Prevent the Audit**. In the event an entity does not respond to an OCR request (i.e., contact verification, pre-screening questionnaire; document request), OCR will use publicly-available information about the entity to create an audit pool. It also could subject the entity to a compliance review.

For more details regarding OCR's 2016 Phase 2 Audit Program, visit OCR's HIPAA Privacy, Security, and Breach Notification Audit Program website.

Should you have any questions regarding OCR's Phase 2 HIPAA Audit Program or should you receive correspondence from OCR regarding the Phase 2 Audit Program, please contact any of the authors of this Client Alert, any members of the Health Law Team, the Privacy and Information Security Team or your regular Baker Donelson contact.