What's New in the Second Phase of OCR HIPAA Audits

BY JOY KOSIEWICZ

THE SECOND PHASE of HIPAA audits is now in process. In 2012, the Office of Civil Rights (OCR) completed the first phase of audits. Phase 1 was a pilot program to assess covered entity compliance with HIPAA. OCR developed enhanced audit protocols based on its experience in Phase 1. These protocols will be used to conduct the Phase 2 audits.

In Phase 2, OCR will target business associates. Covered entities will also be audited, but a key product of Phase 2 will be a business associate database. Although the HITECH rule brought business associates under the authority of OCR, business associates have been difficult to identify and thus have stayed largely out of OCR's radar. Identifying business associates is challenging because of the vast numbers of companies providing covered services. With the growing number of electronic data analysis, storage and transmittal products, these numbers continue to rapidly increase. OCR has solved this conundrum by asking covered entities to provide OCR with a list of their business associates including contact information. OCR can then use the business associate database to create its audit pool.

If you are a covered entity, you will need to have contracts in order for ready identification of business associates. You also need to be prepared for your own audit. OCR will be testing the effectiveness of desk audits using OCR's new secure audit portal. Covered entities will first be contacted by email to verify their contact information. Check your spam and junk mail folders. You cannot avoid an audit by failing to respond to the email. Non-responders will be identified through publicly available information. Following the initial email will be a pre-audit questionnaire to assess each covered entity's size and operations and to collect information on business associates. Auditees will be randomly chosen from pools created using the pre-audit questionnaire.

For business associates, this means you need to be prepared for a HIPAA Audit. Phase 2 will focus on your security measures and your compliance with specific requirements of the privacy, security and breach notification rules. You will be required to submit your current risk analysis, risk management plan, and all applicable policies and procedures.

Both covered entities and business associates must be able to document HIPAA compliance throughout their entire organization, including affiliates. Business associate agreements must be in place and HIPAA compliant. Earlier this month OCR entered into two resolution agreements resulting in over five million settlement dollars. One case involved a business associate that the covered entity did not have a business associate agreement with. Both resolutions cited the covered entity for failure to conduct an adequate risk analysis of its organization-wide information technology infrastructure.

Of note, the Office of Inspector General (OIG) 2016 Workplan promises to review OCR's oversight of the security of electronic protected health information. OCR is responsible for ensuring that both covered entities and business associates are adequately protecting electronic protected health information. OIG audits of OCR found that OCR's oversight has not been adequate, specifically noting that OCR has not implemented periodic audits. OCR has answered by commencing this second round of audits. The desk audits will be completed by December 2016. Following the desk audits, OCR may conduct more extensive onsite audits.

Joy Kosiewicz is a Partner in the Health Care Practice Group of Brouse McDowell in Akron, Ohio. ■