Cooley

OCR Begins Phase 2 of HIPAA Audit Program

March 29, 2016

On March 21, 2016 the US Department of Health and Human Services Office for Civil Rights (OCR) announced the start of phase 2 (Phase 2) of the Health Insurance Portability and Accountability Act (HIPAA) **Audit Program**. OCR outlined that the 2016 Phase 2 HIPAA Audit Program will evaluate the compliance of both covered entities and their business associates with the requirements of the Privacy, Security, and Breach Notification Rules.

The Health Information Technology for Economic and Clinical Health Act (HITECH) requires OCR to conduct periodic audits of covered entities and business associates to determine their compliance with HIPAA. OCR implemented a pilot program in 2011 (Phase 1) in which it evaluated approximately 115 covered entities to determine their compliance with HIPAA over 2011 and 2012. These Phase 1 audits were largely an information gathering and compliance improvement exercise. OCR used the audit reports to ascertain what types of technical assistance should be developed and what types of corrective action are most effective, rather than as a basis for enforcement. A **compliance report** issued last year sheds light on what covered entities and business associates can expect from OCR going forward. OCR is ramping up its efforts and will soon begin its second round of compliance audits, known as Phase 2 HIPAA audits.

OCR notes on its **website** that Phase 2 HIPAA Audits have already started. OCR is currently verifying contact information and sending initial emails to potential subjects with a pre-audit questionnaire that will gather data about the "size, type, and operations of potential auditees." Based on pre-audit questionnaires, OCR will choose the final pool of auditees and send letters shortly. Any covered entity or business associated may be selected for an audit even if they do not respond to OCR's request for pre-audit questionnaires.

OCR has stated that it is "committed to transparency about the process" and will post on its website updated audit protocols that have been developed based on the Phase 1 HIPAA Audits. Phase 2 Audits will include both desk and on-site audits for covered entities and their business associates. OCR is pursuing a new strategy to test the efficiency of desk audits. The first round of Phase 2 HIPAA Audits will be desk audits followed by a round of desk audits of business associates. A third round of audits will result in a select group of subjects of round one or two audits to receive on-site audits.

Once a covered entity or business associate receives a request for a desk audit, they will have 10 business days to respond to the request for documentation. Auditors will review the documentation and provide draft findings. Subjects of the audit will then have 10 days to review the findings and return written comments, if desired. If an on-site audit is required, auditors will schedule a date and provide information about the process. On-site audits will last three to five days. Like desk audits, auditees will have 10 days to review the findings from the audit and return written comments if any.

More serious compliance reviews may be triggered if audits uncover serious compliance issues. Based on the results of the further compliance reviews, covered entities and business associates may be liable for penalties.

Proactive HIPAA and HITECH compliance efforts can ensure that your organization is able to successfully complete a potential OCR audit and mitigate the risk of future losses due to HIPAA and HITECH violations and breaches. Covered entities and business associates should ensure that all HIPAA policies and procedures are up to date and in compliance with of HIPAA. Cooley's Health Care Team has prepared an Audit Toolkit that can assist clients in assessing compliance with HIPAA and HITECH

and determine areas for improvement. Contact us for further information on this topic.