THE
NATIONAL LAW REVIEW

OCR Launches 2016 Phase 2 HIPAA Audit Program

Drinker Biddle
Article By
Stephen A. Serfass
Nolan B. Tully
Christopher F. Petillo
Steven H. Brogan
Drinker Biddle & Reath LLP
Insights

- Communications, Media & Internet
- Health Law & Managed Care

- All Federal

Wednesday, March 30, 2016

On March 21, ***OCR*** announced that it has officially launched its long-anticipated 2016 ***Phase 2 HIPAA Audit Program*** (rumors and unofficial reports of progress on this program have been circulating in recent months). This announcement follows a series of actions demonstrating OCR's escalated focus on HIPAA enforcement in the wake of two recent OIG reports criticizing OCR's enforcement efforts.

Phase 2 Audit Program

Phase 2 will begin with data gathering exercises, followed by targeted "desk audits" (*i.e.*, reviews of organizations' privacy and security compliance policies and procedures) in 2016 and more comprehensive on-site audits starting in 2017. First, OCR will gather data about the size, type, and operations of potential auditees through the use of a pre-audit questionnaire. OCR plans to use the data to create potential audit subject pools (particularly for its plan to audit business associates).

Once the data collection phase is complete, OCR will implement desk audits. These audits will be targeted, focusing on particular Privacy, Security, or Breach Notification Rules. The 2016 desk audits will include covered entities and business associates.

Finally, according to the OCR's Q&A on the new audit program, on-site audits will be

more comprehensive and are scheduled to begin in 2017, after the desk audits are completed (desk auditees may or may not become on-site auditees). Audit results will not be publicized by OCR, but any resulting compliance investigation could become public. Notifications regarding audits are to be distributed by email – so check your inbox!

Recent OCR Enforcement Action

OCR's Phase 2 announcement comes in the wake of substantial resolution agreements related to OCR's compliance investigations. First, on March 16, 2016, OCR announced a $1.5 million resolution agreement with North Memorial Health Care of Minnesota for failing to execute business associate agreements, among other alleged HIPAA violations. Then, just one day later, OCR announced that it reached a $3.9 million settlement with the Feinstein Institute for Medical Research ("Feinstein"), a New York not-for-profit biomedical research institute, over alleged HIPAA violations. The resolution agreement reached with Feinstein is particularly illustrative of the fact that OCR has ratcheted up its enforcement efforts.

The investigation into Feinstein's HIPAA compliance policies and procedures began after Feinstein reported that a laptop containing the electronic protected health information (ePHI) of approximately 13,000 patients and research participants was stolen from the back seat of an employee's vehicle. OCR concluded that Feinstein violated the HIPAA Privacy and Security Rules when it: (1) failed to conduct an accurate and thorough risk assessment; (2) failed to implement policies and procedures for granting access to ePHI by its workforce members; (3) failed to implement physical safeguards for laptops; (4) failed to implement policies and procedures that govern receipt and removal of ePHI into and out of a facility; and (5) failed to implement a mechanism to encrypt ePHI or, alternatively, document why encryption was not reasonable and appropriate and implement an equivalent alternative.

Pursuant to the settlement, Feinstein must implement a corrective action plan including, for example, working with HHS to conduct a risk assessment and risk management plan, reviewing and revising its current privacy and security rules policies and procedures annually to ensure compliance with HIPAA, and training and monitoring its employees to ensure compliance with the revised policies and procedures.

Phase 2 and the Feinstein resolution agreement exemplify OCR's increased appetite for HIPAA enforcement activity in 2016. Thus, OCR's efforts serve as a reminder of the importance of maintaining a culture of compliance and having the architecture in place to efficiently respond to more proactive and searching enforcement activity.