Health Care Alert: OCR Ends 2015 with Announcement of Additional HIPAA Settlements

CLIENT ALERT | 1.4.2016

Recently the Department of Health and Human Services Office for Civil Rights (OCR) announced three settlements to resolve investigations into potential violations of the Health Insurance Portability and Accountability Act (HIPAA).

OCR reached settlements with two academic medical centers, the Lahey Hospital and Medical Center and University of Washington Medicine (UWM), and one insurance holding company, Triple-S Management Company. Each entity will be subject to a corrective action plan and civil monetary penalties that range from $750,000 to $3.5 million.

The Lahey investigation involved a breach of 599 individuals' protected health information (PHI) when an unencrypted laptop was stolen from a workstation. OCR identified several problems with the Lahey compliance program, including a failure to conduct an appropriate risk analysis of electronic protected health information (ePHI), failure to implement proper physical safeguards for the workstation, and a failure to require unique user identities and track users accessing the workstation.

The Triple-S investigation involved a series of five large data breaches each affecting over 500 individuals and two smaller data breaches each affecting less than 500 individuals. OCR found that Triple-S had a culture of non-compliance throughout the parent company and its affiliates. The significant failures within Triple-S's compliance program included a lack of administrative, physical, and technical safeguards to protect PHI, a failure to conduct an adequate risk analysis of all applications using ePHI, and impermissible use or disclosure of PHI to outside vendors and within mailings.

The UWM investigation involved a breach of approximately 90,000 individuals' ePHI after an employee fell prey to a phishing email and opened an attachment containing malware. This is the first settlement action arising from an investigation into a breach from a phishing email. OCR found that UWM had adequate written security policies in place, but failed to ensure that all affiliated facilities where PHI was stored or accessed conducted appropriate risk analyses and additionally failed to include all technological applications

Although the three settlements involved different types of a breach, a common theme running through each of OCR's resulting investigative reports is that the covered entity failed to perform a comprehensive risk analysis. Each of the entities had a risk analysis that was deficient in scope because either the entity failed to properly include every affiliated facility in the risk analysis or because the risk analysis did not include all of the systems and technologies where ePHI was created, transferred, stored, or received. To ensure compliance with HIPAA and HITECH regulations, covered entities should perform a broad risk analysis that covers all possible sources of PHI and keep the risk analysis up to date should any changes be

made within the organization.

Maintaining compliance with HIPAA regulations will likely be even more important in the upcoming year in light of a report the Office of the Inspector General (OIG) issued in October which called for stronger, more proactive oversight from OCR. Notably, within the report the OIG found that more than half of the entities that faced OCR investigations had been deficient in at least one privacy standard. In its response to the OIG report, OCR agreed with the recommendation that its enforcement action should be increased and noted that it would be implementing Phase 2 of a permanent audit program beginning in 2016.

As a result of the OIG's report, covered entities and their business associates should be aware of an increased possibility of a HIPAA Privacy Rule audit or other enforcement activity from OCR. Covered entities should ensure that their HIPAA Security and Privacy policies are both up to date and actually implemented and that comprehensive risk analyses covering all affiliated facilities and sources of PHI have been performed. The full text of the Leahy settlement can be accessed here. The full text of the Triple-S settlement can be accessed here. The full text of the UWM settlement can be accessed here.

The full text of the OIG report can be found here. If you have any questions regarding HIPAA compliance or the need to conduct a risk assessment, please contact your Vorys health care attorney.