Three Recent OCR Actions Demonstrate That HIPAA Enforcement Is Alive and Well

March 23, 2016

Within the past several days, the Office for Civil Rights ("OCR") signaled enhanced HIPAA enforcement on several fronts. First, it initiated Phase 2 of HIPAA compliance audits as mandated by the Health Information Technology for Economic and Clinical Health Act ("HITECH"). Any covered entity or business associate is a possible audit target. Secondly, OCR announced two major settlements with HIPAA covered entities. For these two covered entities that were already the subject of OCR investigations long before the Phase 2 audits started, two stolen laptops generated a total of $4.4 million in HIPAA enforcement costs. These OCR actions demonstrate that the risk of HIPAA non-compliance is serious and real.

Phase 2 Audits

On March 21, 2016, OCR launched Phase 2 of the audits mandated by HITECH. Per OCR, "In its 2016 Phase 2 HIPAA Audit Program, OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted. OCR's audits will enhance industry awareness of compliance obligations and enable OCR to better target technical assistance regarding problems identified through the audits. Through the information gleaned from the audits, OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches."

Per industry sources, OCR will not overlook significant violations revealed during an audit. These could lead to in-depth investigations, settlements, or sanctions.

Right now, OCR is communicating by email with covered entities and business associates to confirm contact information. It will send follow-up emails seeking additional information that it will use to select its audit targets. OCR cautions, however, that failure to respond to its emails will not shield an organization from being included in an audit. OCR advises covered entities and business associates to be alert for email communications from it, including checking spam filters.

Any organization that receives any email communication from OCR would be well advised to immediately conduct an internal review of its HIPAA compliance and promptly fix any potential deficiencies that the internal review may reveal. This will put the organization in the best posture to emerge unscathed from an actual OCR audit if they are a selected target.

North Memorial Health Care

On March 16, 2016, OCR announced a $1.55 million settlement with North Memorial Health Care of Minnesota for failing to comply with what OCR called "two cornerstones" of HIPAA:

- Failure to execute a business associate agreement; and
- Failure to perform a "comprehensive security risk analysis."

The problems came to light after North Memorial Health Care notified OCR that "an unencrypted, password-protected laptop was stolen from a business associate workforce member's locked vehicle, impacting the electronic protected health information (ePHI) of 9,497 individuals." In addition to paying the settlement amount, North Memorial Health Care entered into a compliance agreement requiring it to conduct the missing security risk analysis, sign business associate agreements, modify its policies and procedures, train staff, and periodically report compliance progress to OCR.

Feinstein Institute for Medical Research

Only one day later on March 17, 2016, OCR announced a $3.9 million settlement with Feinstein Institute for Medical Research, described by OCR as a clinical research institute "sponsored by Northwell Health, Inc., formerly known as North Shore Long Island Jewish Health System, a large health system headquartered in Manhasset, New York that is comprised of twenty one hospitals and over 450 patient facilities and physician practices."

Similar to North Memorial Health Care, Feinstein's HIPAA troubles began when it notified OCR that "a laptop computer containing the electronic protected health information of approximately 13,000 patients and research participants was stolen from an employee's car. The Protected Health Information stored in the laptop included the names of research participants, dates of birth, addresses, social security numbers, diagnoses, laboratory results, medications, and medical information relating to potential participation in a research study."

OCR alleged that Feinstein's "security management process was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity. Further, Feinstein lacked policies and procedures for authorizing access to ePHI by its workforce members, failed to implement safeguards to restrict access to unauthorized users, and lacked policies and procedures to govern the receipt and removal of laptops that contained ePHI into and out of its facilities. For electronic equipment procured outside of Feinstein's standard acquisition process, Feinstein failed to implement proper mechanisms for safeguarding ePHI as required by the Security Rule."

In addition to paying the $3.9 million settlement, Feinstein agreed to a corrective action plan that includes conducting a robust security risk analysis, modifying policies and procedures, and training staff.

Lessons Learned

Some HIPAA covered entities may have been lulled into HIPAA compliance complacency because of what may have seemed like limited HIPAA enforcement in the past. These two multimillion dollar settlements indicate that OCR is now extracting serious money for HIPAA violations. The dollar amounts of these settlements are among the largest that OCR has obtained to date. These cases also demonstrate that even in the current climate of concern about high-tech hacking incidents, serious HIPAA sanctions can arise from very low-tech violations. In both cases, the trigger event was theft of a laptop from a car. Covered entities and business associates alike would be well advised to revisit their policies about control of all kinds of mobile devices—laptops, tablets, smart phones, flash drives—which OCR has long identified as high risk. And finally, these settlements reinforce the importance of comprehensive and in-depth security risk analyses which honestly search for vulnerabilities to the confidentiality, integrity and availability of ePHI, coupled with internal corrections and controls to address identified risks.

To learn more about the impact of these recent OCR actions, please contact the author of this alert, **Joanne Lax** at 248-203-0816, any of the attorneys listed to the left or your Dykema relationship attorney.

Attorneys

Amy M. Christen

Jonathan S. Feld

Practice Areas

Health Care

HIPAA—Health Information Privacy & Security

Privacy and Data Security