

OCR ANNOUNCES LARGEST SINGLE-ENTITY SETTLEMENT TO DATE

On August 4, the Office for Civil Rights ("OCR") **announced** a \$5.55 million settlement with the largest fully integrated health care system in Illinois. The settlement is the largest HIPAA settlement ever by a single entity and follows two recent settlements with university health systems in Oregon and Mississippi that were \$2.7 million and \$2.75 million, respectively. In total, OCR has reached nine HIPAA settlements in 2016, in addition to the imposition of civil monetary penalties in another case. This is a significant increase in HIPAA enforcement as OCR entered into only six settlements in all of 2015.

The recent Illinois health system settlement resulted from OCR investigations after the system notified OCR of three breaches between August 23, 2013 and November 1, 2013, which included: (1) the theft of four desktop computers containing the unsecured electronic protected health information ("ePHI") of nearly 4 million individuals; (2) the potential compromise of the ePHI of 2,000 individuals due to unauthorized access to the network of one of the health system's Business Associates; and (3) the theft from a workforce member's car of an unencrypted laptop containing the unsecured ePHI of 2,200 individuals. OCR noted that the health system failed to conduct an enterprise-wide risk analysis incorporating all of the system's facilities, IT equipment, applications and data systems utilizing ePHI; failed to implement appropriate safeguards for ePHI; and failed to enter into a Business Associate Agreement ("BAA") with the billing services company that experienced improper network access.

The corrective action plan entered into by the Illinois system is a useful guide to the type of HIPAA compliance efforts OCR expects to see. The corrective action plan (available [here](#)) requires the system to:

- Conduct an enterprise-wide risk analysis and develop an enterprise-wide risk management plan;
- Implement a process for evaluating changes to the operations and security environment of the enterprise;
- Develop a report on enterprise-wide encryption status, including an explanation for the total number of devices and equipment that are not encrypted;
- Review and revise policies on device and media controls and facility access controls;
- Review and revise policies on business associates;
- Develop an enhanced privacy and security training program for all workforce members; and
- Develop a plan to internally monitor its compliance with the plan and engage an external, third-party monitor to periodically assess its adherence to the plan's numerous requirements.

Although these recent large settlements have involved large health care providers, medium and small providers also need to ensure that they are conducting a comprehensive risk analysis, timely addressing vulnerabilities and entering into BAAs. With Phase 2 HIPAA desk audits in full force for 167 entities, OCR is sending a strong and timely message to HIPAA Covered Entities and Business Associates. In light of this, Covered Entities and Business Associates should take the necessary steps to ensure their HIPAA compliance programs are effective to protect health information and avoid potentially large penalties.

If you need additional information about this topic or Hall Render's HIPAA audit services, please contact:

- Mark Swearingen at 317-977-1458 or mswearingen@hallrender.com;
- Tony Caldwell at 317-977-1469 or acaldwell@hallrender.com; or
- Your regular Hall Render attorney.

View this article and other health law-related posts by visiting the Hall Render Blog at: <http://blogs.hallrender.com> or click [here](#) to sign up to receive Hall Render alerts on topics related to health care law.