HINSHAW

Two New York Hospitals Enter Into Largest Ever HIPAA Settlement After Electronic Data Breach

Healthcare Alert | 3 min read
May 12, 2014

The federal government is becoming more aggressive in pursuing HIPAA breaches, as indicated by a $4.8 million settlement entered into between the Office of Civil Rights (OCR) of the Department of Health and Human Services and two New York-based health care organizations. In the largest HIPAA settlement to date, New York Presbyterian Hospital has paid $3.3 million and Columbia University has paid $1.5 million to OCR, and both entities have agreed to a corrective action plan for a data breach involving the failure to secure approximately 6,800 patients' electronic protected health information (ePHI). The breach was discovered after an individual found information about his deceased partner on the internet. His partner was a former patient of New York Presbyterian. The joint settlement is the largest monetary sum paid to date for a HIPAA violation and demonstrates the importance of compliance with the security provisions of HIPAA, which include conducting risk assessments, ensuring that ePHI is secured, addressing the potential risks of errors in server configuration, knowing each and every system that has access to ePHI, and ensuring that staff have proper training.

New York Presbyterian and Columbia are separate covered entities that participate in a joint arrangement in which Columbia faculty member physicians serve as attending physicians at New York Presbyterian. As part of this affiliation, called New York Presbyterian Hospital/Columbia University Medical Center, the entities operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to New York Presbyterian patient information systems containing patient ePHI.

In September 2010, the entities submitted a joint data breach report to OCR after they received a complaint that records of New York Presbyterian patients were accessible on the internet. OCR conducted an investigation that determined that the medical records of approximately 6,800 patients of New York Presbyterian were accessible on the internet and obtainable though Google and other internet search engines. The information available on the internet included patient status, vital signs, medications, and laboratory results. The breach occurred when a physician employed by Columbia who had developed software applications for both entities attempted to deactivate a personally owned computer server on the New York Presbyterian internal data network. In the course of its investigation, OCR also found that neither organization had made efforts prior to the breach to

assure that the server was secure or contained appropriate software protections. According to OCR, neither entity had developed an adequate risk management plan that addressed the accessibility of ePHI or had addressed the potential threats and hazards to the security of the ePHI. Further, OCR found that New York Presbyterian failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management. Despite the fact that New York Presbyterian takes the position that there is no proof any of the records were accessed or used inappropriately, OCR found that the parties had violated HIPAA and sought penalties and corrective action. Further, although the breach dealt with access to New York Presbyterian ePHI, OCR determined that Columbia still had responsibility for the security breach, since it participated in a joint data sharing arrangement with New York Presbyterian and therefore shared responsibility for the security of the data. See U.S. Department of Health & Human Services, *Data breach results in $4.8 million HIPAA settlements,* (May 7, 2014),

This case underscores the importance of implementing and repeatedly updating data security measures, and the essential role of IT in developing and implementing HIPAA policies and procedures. All covered entities and business associates need to: (i) conduct thorough, complete and accurate risk analyses on an ongoing basis and address identified threats and vulnerabilities and document such efforts; (ii) develop and enforce policies and procedures on access to and the security of servers; (iii) ensure that technical safeguards are in effect for servers; and (iv) conduct staff training on security issues. Covered entities and business associates are responsible for knowing all of the systems, IT equipment, applications and data systems that can access ePHI, and for monitoring updates to their servers as well as monitoring unauthorized access to ePHI. And, they are responsible for the security of data involved in joint data sharing arrangements.

Should you have any questions or need further information, please contact your regular Hinshaw attorney.