THE
NATIONAL LAW REVIEW

Electronic Data Breach Leads to Largest Health Insurance Portability and Accountability Act (HIPAA) Settlement to Date

Article By
Molly Nicol Lewis
McBrayer, McGinnis, Leslie and Kirkland, PLLC
Health Care Law Blog

- Insurance Reinsurance & Surety
- Consumer Protection
- Communications, Media & Internet
- Health Law & Managed Care
- Administrative & Regulatory

- All Federal

Tuesday, May 27, 2014

Recently, the **Office of Civil Rights ("OCR")** of the Department of Health and Human Services entered into a $4.8 million dollar settlement with two New York-based health care organizations after a data breach involving electronic protected health information occurred. The agreement is the largest HIPAA settlement thus far.

New York and Presbyterian ("NYP") and Columbia University ("CU") are covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. 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 NYP patient information systems containing ePHI.

After receiving a complaint that records of NYP patients were accessible on the internet in 2010, NYP and CU submitted a joint breach report. OCR subsequently conducted an investigation and found that the medical records (including patient status, vital signs, medications, and lab results) of 6,800 NYP patients were accessible on the internet. The investigation revealed the breach occurred when a

physician employed by CU attempted to deactivate a personally-owned computer server on the NYP internal data network. Because of a lack of technical safeguards, deactivation of the server resulted in widespread, accessible ePHI.

Not only did OCR find an impermissible disclosure of ePHI, but they also found that neither entity made efforts prior to the breach to assure that the server was secure and contained appropriate software protections. Further, neither entity had conducted a risk analysis or addressed the threats and hazards to the security of the ePHI. NYP failed to implement appropriate policies and procedures for authorizing access to its database and failed to comply with its own policies on information access management. NYP and CU were required to pay $3,300,000 and $1,500,000, respectively. Both entities agreed to a substantive corrective action plan.

This settlement reaffirms what health care attorneys have repeatedly emphasized – covered entities must conduct thorough risk analysis and specifically analyze the technical, physical, and administrative safeguards in place to protect ePHI. Collaborative entities, like NYP and CU, must be jointly responsible for developing and implementing policies, training staff, and monitoring ePHI access. All entities should work closely with IT to ensure that their systems are HIPAA-compliant.

Source URL: https://www.natlawreview.com/article/electronic-data-breach-leads-to-largest-health-insurance-portability-and-accountabil