News

FOR IMMEDIATE RELEASE
May 7, 2014

Contact: HHS Press Office
(202) 690-6343

Data breach results in $4.8 million HIPAA settlements

Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center." NYP and CU 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.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.

In addition to the impermissible disclosure of ePHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP 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.

"When entities participate in joint compliance arrangements, they share the burden of addressing the risks to protected health information," said Christina Heide, Acting Deputy Director of Health Information Privacy for OCR. "Our cases against NYP and CU should remind health care

organizations of the need to make data security central to how they manage their information systems."

NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports.

For information about the basics of HIPAA Security Risk Analysis and Risk Management, as well as other compliance tips, visit: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training

The New York and Presbyterian Hospital Resolution Agreement may be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf

The Columbia University Resolution Agreement may be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/columbia-university-resolution-agreement.pdf

To learn more about non-discrimination and health information privacy laws, your civil rights and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at www.HHS.gov/OCR

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: May 8, 2014