CORPORATE COMPLIANCE ALERT

5/14/14

Two Prominent New York Health Care Organizations to Pay Record-Setting HIPAA Fine of $4.8 Million

By **Brian E. Dickerson**

New York Presbyterian Hospital (NYP) and Columbia University (CU) have agreed to pay a combined $4.8 million to settle allegations that they failed to secure the electronic protected health information (ePHI) of thousands of patients, making the settlement the largest to date for violations of the Health Insurance Portability Act's (HIPAA) privacy provisions regarding patient records. The sizeable settlement was agreed upon despite the fact that the violation was self-reported by NYP/CU, and there was no indication at the time, nor subsequently, that the ePHI had been accessed or used inappropriately.

NYP and CU, collectively referred to as "New York Presbyterian Hospital/Columbia University Medical Center" by virtue of a joint arrangement in which Columbia University faculty members serve as attending physicians at New York Presbyterian, operate a shared data network and firewall that is administered by employees of both institutions. NYP and CU submitted a joint breach report in late September 2010, disclosing to the U.S. Department of Health and Human Services (HHS) that the ePHI of 6,800 NYP/CU patients had been compromised. The ePHI included patient status, vital signs, medications and laboratory results.

An investigation by the HHS Office for Civil Rights (OCR) revealed that the breach occurred when a CU physician who developed applications for both NYP and CU attempted to deactivate a personally owned computer server on the network containing NYP patient information. The server deactivation left the ePHI data accessible via internet search engines.

The OCR investigation ultimately determined that:

- Neither NYP nor CU made efforts prior to the breach to assure that servers were secure and contained appropriate software protections;
- Neither NYP nor CU had conducted an accurate and thorough risk analysis that identified all systems that accessed NYP ePHI data;
- Neither NYP nor CU had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI data;
- NYP failed to implement appropriate policies and procedures for authorizing access to its databases; and
- NYP failed to comply with its own policies on information access management.

As a part of the settlement agreement with HHS and in addition to the $4.8 million fine, both NYP and CU must undertake a risk analysis, develop risk management plans, revise policies, train staff and provide HHS with progress reports.

As noted by Christina Heide, Acting Deputy Director of Health information Privacy for OCT, “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.”

Roetzel’s white-collar litigation and corporate compliance attorneys are available to assist you with any questions regarding the establishment, implementation and ongoing maintenance of a HIPAA and ePHI compliance program. Please contact the following Roetzel attorneys for further information:

Anthony J. Calamunci
419.254.5247 | acalamunci@ralaw.com

Brian E. Dickerson
202.570.0248 | bdickerson@ralaw.com

James L. Ervin, Jr.
614.723.2081 | jervin@ralaw.com

Saqib Ishaq
407.839.2749 | sishaq@ralaw.com

Thomas M. Larned
202.697.4892 | tlarned@ralaw.com

Donald S. Scherzer
216.615.7418 | dscherzer@ralaw.com

Rose M. Schindler
954.759.2751 | rschindler@ralaw.com

Jonathan R. Secrest
614.723.2029 | jsecrest@ralaw.com

Nicole Hughes Waid
202.906.9572 | nwaid@ralaw.com

Amanda M. Knapp
216.615.7416 | aknapp@ralaw.com