CORPORATE COMPLIANCE ALERT

11/13/13

Expanded HIPAA Privacy Rules Impose Requirements on Non-Healthcare Businesses in Possession of Medical Records

On September 23, 2013, tough new privacy regulations under the Omnibus Final Rule (Omnibus Rule) update to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) went into effect. Healthcare providers and others that fall under the category of healthcare Business Associates (BA) can expect increased levels of enforcement by both state and federal authorities.

The Omnibus Rule greatly expands the number of organizations directly responsible for compliance with HIPAA privacy regulations. The requirements of the Omnibus Rule make BAs liable for failure to secure Protected Health Information (PHI), a rule that previously applied only to healthcare providers. Under the Omnibus Rule, a BA is a person or entity that provides services to or on behalf of a covered healthcare provider, and, in the course of providing such services, has access to the covered entity's PHI. The list of affected BAs may include any number of vendors, contractors or consultants, including those providing professional services, e.g., attorneys, accountants, marketers or software vendors.

The penalties per violation range from $100 to $50,000, depending in part on whether the violation was caused by ignorance or willful neglect, with a maximum penalty of $1.5 million. Penalties for some violations may also include significant prison terms, as demonstrated by the recent sentencing of a Florida health care worker to three years in prison and a $12,000 fine for stealing and selling HIPAA protected patient information. The U.S. District Court for the Middle District of Florida imposed the lengthy prison term despite the fact that the defendant, through her efforts to sell social security numbers, birth dates and other information, received little money. According to the U.S. Attorney's Office, federal prosecutors sought the stiff penalty to make an example of the defendant as a symbol of an increasingly common type of criminal. Further, in order to increase enforcement, the Omnibus Rule provides that State's Attorneys General, in addition to the Office for Civil Rights at the Department of Health and Human Services (HHS), may pursue civil actions against those accused of HIPAA violations.

According to HHS[1], the issues that will most frequently lead to a formal investigation include:

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Uses or disclosures of more than the minimum necessary protected health information; and
- Lack of administrative safeguards of electronic protected health information.

Further, the entities most commonly required to take corrective action to achieve compliance are[2]:

- Private Practices;
- General Hospitals;
- Outpatient Facilities;

[1] U.S. Department of Health & Human Services http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html
[2] *Ibid*.

- Health Plans; and
- Pharmacies.

With the inclusion of BAs to the list of entities now required to comply with HIPAA privacy rules, it remains to be seen what additional types of businesses may find themselves required to take corrective actions in order to achieve compliance.

In order to avoid potential civil and criminal liability issues related to the new privacy regulations, both healthcare entities and their BAs and subcontractors should undertake a thorough internal compliance review and a review of all BA contracts and agreements. Further measures may include revisions to written policies and procedures and employee retraining.

For further information on HIPAA compliance under the new requirements of the Omnibus Rule, please contact the following Roetzel attorneys:

Lynn M. Barrett
954.759.2768 | lbarrett@ralaw.com

Edgar Asebey-Birkholm
954.759.2754 | easebey@ralaw.com

Anthony J. Calamunci
419.254.5247 | acalamunci@ralaw.com

Alan H. Daniels
407.245.2426 | adaniels@ralaw.com

Brian E. Dickerson
202.570.0248 | bdickerson@ralaw.com

Ned Milenkovich
312.582.1676 | nmilenkovich@ralaw.com

Rose M. Schindler
954.759.2751 | rschindler@ralaw.com

James Schuster
216.820.4231 | jschuster@ralaw.com

Jonathan R. Secrest
614.723.2029 | jsecrest@ralaw.com

Andrew S. Feldman
954.759.2753 | afeldman@ralaw.com

Amanda M. Knapp
216.615.7416 | aknapp@ralaw.com