CLIENT ADVISORY – HEALTH CARE LAW

HIPAA Breach Notification Analysis Under the Omnibus Rule

July 2, 2014

The final Omnibus Rule ("Rule"), effective March 26, 2013, modified the HIPAA Privacy and Security Rules and increased the burden on Covered Entities[i] and Business Associates[ii] in the area of breach notification.

While the government reiterated that encryption remains a safe harbor, the Rule materially changed the approach to determining whether an inappropriate use or disclosure of protected health information ("PHI") constitutes a reportable breach. Whereas the prior standard focused on whether an inappropriate use or disclosure posed a significant risk of harm to the individual, the new standard presumes all inappropriate uses or disclosures to be reportable breaches, unless the Covered Entity or Business Associate can demonstrate a low probability that the PHI has been compromised. This includes an analysis of the following four factors:

(1) Nature and extent of PHI involved, including the possibility of re-identification and the types of identifiers in question;

(2) Nature of the person who used or received the PHI without authorization, including whether the recipient has confidentiality obligations;

(3) Extent to which PHI was in fact accessed, as opposed to whether there was merely opportunity to acquire or view the information; and

(4) Extent to which the Covered Entity or Business Associate has mitigated the risk, for example through a confidentiality agreement from the recipient.

Additionally, the Rule indicates that Covered Entities and Business Associates can consider other unnamed factors in addition to the above in performing the breach analysis obligations. Also, the Rule indicates that a violation of the minimum necessary standard – which requires reasonable efforts to limit any use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request – could be grounds for a breach notification.

In the case of a Business Associate performing services for a Covered Entity that involves use or access of PHI, the Rule requires the Business Associate notify the Covered Entity when it discovers a breach of unsecured PHI without unreasonable delay and in no case later than 60 days after the discovery of the breach.

The government has announced intentions to focus future audit activity of Business Associates on the breach notification process, and to focus future audit activity of Covered Entities on the content and timeliness of breach notifications. Therefore, it is imperative for both Covered Entities and Business Associates to have thorough and consistent processes in place for reporting of inappropriate uses and disclosures, assessing whether such uses and disclosures constitute reportable breaches, providing timely notification with the proper content, and a documentation system that tracks all of the above activities.

We welcome the opportunity to answer any questions you may have regarding the new HIPAA rules or to assist you in assessing your options for complying with those rules.

---

[1] A Covered Entity is a Health Plan, Health Care Clearinghouse, or Health Care Provider which transmits health information in electronic form in connection with a transaction covered by HIPAA Rules.

[2] A Business Associate is a person or entity which performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information on behalf of a Covered Entity.