CLIENT ADVISORY – HEALTH CARE LAW

Government Announces Upcoming HIPAA Audits of Business Associates

June 25, 2014

In the February 24, 2014 Federal Register, the Health and Human Services Office of Civil Rights ("OCR") announced its plans to survey between 550 and 800 entities during the summer of 2014, preparatory to future OCR audits. OCR further clarified in an April 2014 presentation its intention to conduct approximately 400 audits, expected to commence in fall of 2014 after completion of the survey phase.

Of the 400 entities selected for audit, it is anticipated that 350 will be Covered Entities (including 100 health care providers, 45 health plans, and 5 health care clearinghouses) and 50 will be Business Associates (including 35 IT-related Business Associates and 15 non-IT related Business Associates). This is the first time the government will audit Business Associates. Business Associate audits are expected to begin in 2015. It appears OCR intends to focus its audit of Business Associates on proper breach reporting to the Covered Entity, as well as the security risk assessment and risk management process.

The final Omnibus Rule ("Rule") expanded the definition of Business Associates to include, for example, cloud storage providers of protected health information ("PHI"), physical storage providers of PHI, and health information organizations. Under the Rule, a Business Associate is a person or entity that creates, receives, maintains, or transmits PHI to perform certain functions or activities on behalf of a Covered Entity. This also includes subcontractors creating, receiving, maintaining, or transmitting PHI on behalf of a Business Associate. Under the Rule, Business Associates are required to have policies and procedures that comply with HIPAA in the following ways:

(1) Business Associates must enter into current, valid Business Associate Agreements with Covered Entities and with subcontractors handling PHI. Any use, access, or disclosure of PHI done by the Business Associate must be done in accordance with the terms of the Business Associate Agreement;

(2) Business Associates must not impermissibly use or disclose PHI;

(3) Business Associates must provide breach notifications to Covered Entities;

(4) Business Associates must provide access to a copy of ePHI (electronic PHI) to the Covered Entity, individual, or designee as set forth in the Business Associate Agreement;

(5) Business Associates must disclose PHI to the Secretary of Health and Human Services upon request;

(6) Business Associates must provide an appropriate accounting of disclosures; and

(7) Business Associates must comply with the Security Rule by implementing the required administrative, technical, and physical safeguards and maintaining required documentation.

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.

Disclaimer *This Client Advisory has been prepared and published only for informational purposes for clients (and friends) and is not offered, and should not be construed, as legal advice. Because of its generality, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.*