January 23, 2013

HHS Issues New Regulations on HIPAA Privacy and Security

Last week, the Department of Health and Human Services issued final regulations under the Privacy and Security portions of the Health Insurance Portability and Accountability Act (HIPAA). Following is a brief, preliminary summary of major provisions of the regulations of interest to employer group health plan sponsors.

Business Associates. Generally, the HIPAA Privacy and Security rules focus enforcement on covered entities, which are health care providers, health plans, and health care clearinghouses. In addition, the HITECH Act extended many of the HIPAA privacy and security provisions to business associates of covered entities. Under the final rule, business associates and, in certain cases, subcontractors of business associates, are now directly liable for compliance with certain HIPAA requirements.

Breach Notification. The final regulations no longer use *"a significant risk of harm to the individual"* as the standard to trigger a breach notification. Under the final rules, all impermissible uses or disclosures of unsecured protected health information (PHI) are presumed breaches triggering notification, unless the covered entity (or business associate) can demonstrate through a risk assessment that there is a low probability that the PHI was comprised or an exception applies. The final rule then sets out a number of factors to determine whether PHI is compromised, such as the type of PHI improperly used or disclosed.

Notice of Privacy Practices. The final regulations require group health plans to update and redistribute their Notices of Privacy Practices to include, among other things, an explanation of the breach notification requirements.

Increased Enforcement. The civil monetary penalty structure is permanently increased. Increased penalties are based on the level of negligence, with a maximum penalty of $1.5 million per violation.

Genetic Information Nondiscrimination Act (GINA). GINA prohibits the use of genetic information such as family medical history for underwriting purposes. The final rules extend the prohibition on the use or disclosure of genetic information for underwriting purposes to all health plans covered by the HIPAA privacy and security rules, even those to which GINA does not expressly apply. However, long-term care plans are exempt from this prohibition under the final rules.

Effective Dates. The final regulations are effective on **March 26, 2013**, but compliance with certain provisions, *e.g.* breach notifications and GINA, is not required until **September 23, 2013**. Certain business associate agreements may be eligible for additional transition relief through September 23, 2014.

Next Steps. Employer plan sponsors should begin updating their HIPAA Policies and Procedures, Notice of Privacy Practices and business associate agreements to conform to the final rules.

Contact Information. For more information from Mazursky Constantine, please contact Amy Heppner (404.888.8825), Kelly Meyers (404.888.8838), Carl Lammers (404.888.8872) or Jessica Gallegos (404.888.8849). For more information from VCG Consultants, please contact Leslie Schneider (770.863.3617).

IRS Circular 230 Notice: To ensure compliance with requirements of U.S. Treasury regulations, we inform you that any tax advice contained in this newsletter is not intended to be used, and cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code or promoting, marketing or recommending to another party any transaction or matter addressed herein.

999 Peachtree Street • Suite 1500 • Atlanta, GA 30309
www.mazconlaw.com • 404.888.8820
www.VCGConsultants.com • 770.863.3600