October 2013

Is Your Business HIPAA Compliant?

Diane M. Racicot | 619.515.3273 | diane.racicot@procopio.com
Robert G. Marasco | 619.906.5732 | robert.marasco@procopio.com

Many individuals and businesses do not realize they are obligated to comply with the Health Insurance Portability and Accountability Act, better known as HIPAA. This is dangerous, particularly given the increased government scrutiny in this area and the enhanced civil penalties for non-compliance. Moreover, the risks of non-compliance are potentially life-threatening for a company whose business model centers on the provision of services to health care providers and health plans whether directly or through subcontracted arrangements.

The Omnibus HIPAA Final Rule implemented the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009 and it imposed a September 23, 2013 compliance deadline for most of its requirements. While most people now recognize that health care providers such as hospitals and doctors and health plans are subject to HIPAA's requirements, many do not realize that their business relationships have placed them squarely within HIPAA's umbrella as business associates or subcontractors to business associates.

In addition to covered entities such as hospitals, physicians, and plans, HIPAA imposes strict privacy, security and breach notification obligations on individuals and entities that are considered "business associates." The HITECH Act made many aspects of HIPAA directly applicable to business associates. The Final Rule clarifies the manner in which HIPAA applies to business associates (and subcontractors to business associates) and it expands the definition of business associate. If your business creates, receives, maintains or transmits protected health information (PHI) to perform certain functions or activities on behalf of a covered entity, such as claims processing, data analysis, etc., it is likely directly subject to many of HIPAA's privacy, security and breach notification requirements. HIPAA also applies directly to individuals and entities that provide covered entities with professional services that involve the use or disclosure of PHI, such as lawyers, accountants, and consultants, to name a few. The Final Rule also expanded the scope of business associates to include entities that provide data transmission, offer personal health records or maintain PHI (whether physical storage or electronic storage in the cloud) on behalf of covered entities.

As a business associate creating, using, transmitting or maintaining PHI, you will need to ensure your clients that you are HIPAA compliant. Some of your HIPAA obligations include:

- Conducting a risk assessment of your company's physical and technological safeguards.
- Implementing administrative, physical and technical safeguards to protect electronic protected health information.
- Documenting your HIPAA policies and procedures.
- Identifying and implementing policies and procedures to make information available to your covered entity clients in order that they can comply with the individual's rights to access, amendment and accounting of their PHI.
- Identifying, mitigating and reporting disclosures of unsecured PHI.

- Entering into business associate contracts with your clients and subcontractors that contain representations related to the use and disclosure of PHI and your related obligations under HIPAA.

- Updating existing BAAs to reflect the recent changes to the HIPAA.

The government is serious about enforcing HIPAA compliance. It regularly investigates complaints of non-compliance and breaches, conducts audits of covered entities and business associates and imposes penalties for breaches. It is imperative that individuals and entities determine whether they are subject to HIPAA and, if so, that they incorporate HIPAA compliance in their business model. Procopio can help you with that assessment and assist you in identifying and implementing your HIPAA obligations.

Diane M. Racicot focuses her practice on business, compliance, and reimbursement matters for health care providers and suppliers including hospitals, hospices, home health agencies, physician practices, durable medical equipment companies, clinical laboratories, and medical transportation suppliers. Ms. Racicot works with provider, health plan and business associate clients to address state and federal (e.g. Health Insurance Portability and Accountability Act (HIPAA)) health care privacy and security requirements and she provides guidance to assist clients in resolving privacy and security incidents. She helps clients respond to third party subpoenas and other requests for patient records consistent with their privacy law obligations.

Robert G. Marasco serves as medical staff counsel for numerous hospitals and health systems, and also serves as litigation counsel on behalf of health systems, hospitals, physician groups, and individual providers in business, professional liability, fraud and abuse, and administrative matters in both Federal and State court. Mr. Marasco also utilizes his background as a former Assistant United States Attorney to effectively and efficiently defend corporate clients and individuals who are working through complex internal or government investigations, responding to grand jury and administrative subpoenas, or facing criminal prosecution. He also advises clients on compliance with health care laws including fraud and abuse laws, the Health Insurance Portability and Accountability Act (HIPAA) and other health care privacy laws.