GLASER & WEINER, LLP

ATTORNEYS AT LAW

Business Owners Beware… HIPAA is Not Just for Health Care Providers Anymore

Even if your business does not provide health care services, it could still create, receive, maintain, or transmit protected health information (PHI). If so, it may be a "business associate" and it may now have to answer directly to the United States Department of Health and Human Services for violations of HIPAA. The term "business associate" has always covered significant number of vendors that use or disclose PHI in connection with the business relationships they have with health care professionals, also called "covered entities". PHI generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by health care professionals and that can be used to identify an individual, determine appropriate care and track payments.

The recently enacted HIPAA Omnibus Rule expands the scope of the business associate definition even further to include not only those vendors that "create, receive or transmit PHI on behalf of a covered entity," but also those that "***maintain***" PHI on behalf of a covered entity. As a result of the addition of the term "maintain" to the business associate definition, physical and electronic storage facilities as well as other IT companies may now be business associates. If your company provides data storage through the cloud, now is the time to assess your business model. As part of your service, does your company have "routine access" to the PHI data? If so, you are likely going to be swept up in the definition of business associate. Other examples of businesses that can be business associates includes those who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity.

In its original form, HIPAA required covered entities and their business associates to enter into Business Associate Agreements (BAA). This is still the case. However, the new HIPAA Omnibus Rule also requires business associates to enter into BAAs with any organization with whom it subcontracts that performs the functions of a business associate. Among other things, BAAs require business associates and their subcontractors to comply with the HIPAA Privacy and Security Rules, which means that business associates and their subcontractors must have HIPAA compliance policies and procedures in place to address the Security Rule's administrative, physical, and technical safeguards for handling PHI.

The United States Department of Health and Human Services, through its Office of Civil Rights (OCR) now has the right to conduct investigations of business associates and their subcontractors directly regarding their potential violations of HIPAA. Depending on the result of the investigation, OCR may impose up to $1.5 million in civil monetary penalties directly against business associates and/or their subcontractors for each HIPAA violation. Violations may include failing to provide notification to a covered entity of a breach of PHI; making impermissible disclosures of PHI; or failing to account for disclosures of PHI. Criminal penalties may also be imposed.

The HIPAA Omnibus Rule has changed the landscape for covered entities, business associates and subcontractors. Covered entities need to be more diligent in reviewing the operations of their business associates to understand if the business associate works with subcontractors and in making sure the appropriate BAAs are in place. Business associates also need to make sure they have BAAs in place with their subcontractors and review and implement policies and procedures necessary to comply with the HIPAA Omnibus Rule. They should ensure that their subcontractors comply as well.

With the power given to OCR to enforce the law and impose penalties directly against business associates and their subcontractors, failing to assess whether the HIPAA Omnibus Rule applies to your business is not an option.
