Updating HIPAA Compliance Plans & Documents Under the New HIPAA-HITECH Omnibus Rule Regulations

Every entity that participates in the health care sector, whether an independent health care provider, a hospital system, a health care IT vendor, or a health plan, must reevaluate its HIPAA compliance plan in light of the changes enacted by the new HIPAA regulations which went into effect on March 26, 2013. The new regulations, often called the HIPAA-HITECH Omnibus Rule, amends HIPAA's governing regulations to make them compliant with the HITECH Act, including raising the potential level of enforcement penalties to $1.5 million per year per section violated. All Covered Entities, Business Associates, and Business Associate subcontractors need to consider which documents or practices require updating to maintain their HIPAA compliance as the HIPAA requirements continue to evolve with the changing landscape of health care, technology, and privacy. Likely the most critical changes enacted by the new HIPAA regulations are the redefinition and expansion of Business Associates' and their subcontractors' HIPAA responsibilities and the use of agency law to allocate liability and knowledge of HIPAA violations. Subject to certain exceptions, a Business Associate is now defined as a person who creates, receives, maintains, or transmits protected health information in connection with a HIPAA-regulated function or activity, or provides legal, actuarial, accounting, consulting, data aggregation, management, or similar services that involve the disclosure of protected health information. In other words, a Covered Entity's business universe is full of potential Business Associates. The addition of the word "maintains" to the definition clarifies that cloud storage service providers are subject to HIPAA if they maintain protected health information for a Covered Entity or Business Associate. Every participant in the health care market will need to reevaluate their relationships with other health care businesses to ensure that the proper agreements govern their relationship and that they have correctly allocated the compliance responsibilities between the parties as intended. Entities that provide services to Business Associates and were not previously directly subject to HIPAA may now be "subcontractors" under the regulations. Business Associates are required to enter into Business Associate Agreements with all of their subcontractors that handle protected health information. Covered Entities are not required to have any agreements with a Business Associate's subcontractors, but the Business Associate Agreement between a Covered Entity and a Business Associate must require that the Business Associate ensures their subcontractors' compliance through the Business Associate's agreements with its subcontractors. The use of agency law to allocate liability and knowledge of violations means that Covered Entities may be responsible for HIPAA violations by their Business Associates if the Covered Entity has the authority to control the conduct of the Business Associate, other than by termination of a contract. This determination will be made based on the potential control available and will not depend on whether the parties agree that their relationship is not an agency relationship. Further compounding these issues, if a Business Associate is determined to be an agent of a Covered Entity then any knowledge of a HIPAA breach by the Business Associate is imputed to the Covered Entity as of the day the Business Associate learns of the violation. This means that the clock for providing any required notifications to the affected individuals, the Secretary of Health and Human Services, and potentially the media starts ticking as soon as the Business Associate or subcontractor learns of a breach if they are an agent. All of the above rules also apply to the liability of Business Associates with respect to their Business Associate subcontractors. The good news is that the new regulations clarify that a Covered Entity or Business Associate is generally not responsible for a breach by its Business Associates if they are not agents. In light of these changes, it is essential that every Covered Entity and Business Associate know which of their Business Associates and/or subcontractors are their agents to determine both the desired level of

indemnification provided by their contracts and the timeframe in which any breach must be reported. Every business or provider subject to HIPAA must be in compliance with the new rules by September 23, 2013. The documents which must be revised and redistributed by all entities subject to HIPAA include all Business Associate Agreements, the Notice of Privacy Practices, and any related compliance plan documents or guidance. Business Associate Agreements (or other contracts that contain the required Business Associate provisions) that were entered into before January 25, 2013, and are not renewed or modified between March 26 and September 23, 2013, are grandfathered and do not need to be updated until September 22, 2014. However, if a Business Associate Agreement (or other contract) is renewed or modified on or after September 23, 2013, the Business Associate Agreement or other contract must be updated to comply with the new rules at the time of renewal or modification.