Final HIPAA / Hitech Regulations Published: Subcontractors Are Required To Directly Comply With HIPAA

By: Jennifer J. Daniels, Esq.

This is the first in a series of Alerts to be published regarding the Final Rule, titled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules." We will be publishing in the coming days Alerts regarding impacts on Business Associate obligations, breach notice obligations, research, marketing, fundraising, individual access and enforcement.

The long-awaited HIPAA/HITECH Final Rule is out! The Final Rule is effective March 26, 2013, but Covered Entities, Business Associates and Subcontractors will have 180 days beyond the effective date to come into compliance, which 180 days expire on September 23, 2013.

The HITECH Act made a big leap by expanding HIPAA's reach to cover Business Associates directly. But the Department of Health and Human Services (HHS) has taken an equally big leap in now expanding HIPAA's reach to directly cover Subcontractors, a change that was forecasted in the Notice of Proposed Rulemaking that was published in July 14, 2010. Subcontractors are now required to comply with HIPAA and the HITECH Act in the same manner as Business Associates, and are subject to liability and enforcement, including civil monetary penalties, for a failure to comply.

The Final Rule defines a Subcontractor as "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate." The Final Rule also changes the definition of a Business Associate to now include a "subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate." Accordingly, a Subcontractor is directly obligated to comply with the requirements of HIPAA and HITECH, including the HIPAA Security Rule and the breach notification obligations, in the same manner as a Business Associate.

The Final Rule requires Business Associates to enter into agreements with their Subcontractors that include the same terms that have always been required for Business Associate Agreements. Until now, Covered Entities were obligated in their Business Associate Agreements to include a provision that required a Business Associate to ensure that any agents, including subcontractors, to whom the Business Associate disclosed PHI, agreed to the same restrictions and conditions that applied to the Business Associate with respect to such PHI under the Business Associate Agreement. So, Business Associates generally passed along their contractual obligations to their service

providers, but their obligation to do so was contractual. Now, Business Associates have a direct regulatory obligation to enter into agreements with their Subcontractors. A Covered Entity is explicity not obligated to enter into agreements with Subcontractors of its Business Associates. And, the Final Rule and the preamble make clear that the requirements of HIPAA and the HITECH Act apply to a Subcontractor regardless of whether the Business Associate fails to enter into a contract with the Subcontractor. HIPAA's regulatory obligations apply directly to the Subcontractor and not only pursuant to the contract that the Subcontractor has with the Business Associate.

The preamble to the Final Rule also makes clear that the term "Subcontractor" includes those acting on behalf of a Subcontractor, and the requirements apply all the way down the subcontracting chain as far as the PHI flows. So, Covered Entities must ensure that they obtain satisfactory assurances (in the form of a Business Associate Agreement) from their Business Associates, and Business Associates must do the same with regard to Subcontractors, and so on, no matter how far down the chain the PHI flows. Both the contractor and all of the subcontractors are Business Associates under the Final Rule to the extent they create, receive, maintain, or transmit Protected Health Information.

Obligations of a Subcontractor

Service providers must determine whether they are a Subcontractor under HIPAA. HHS does not address the difficulty that companies handling information might face if they never know that they are a Subcontractor handling PHI. For example, a shredding company may enter into an agreement with a customer and receive papers to shred without ever knowing that the papers contain PHI or that its customer is a Business Associate. It is easier for "first tier" service providers that are entering into arrangements with hospitals or insurers to know they are handling health information and that HIPAA might apply. Once information flows downstream, it may be more difficult for service providers to know that they have information that is PHI and that they are, therefore, obligated to comply with HIPAA. This is problematic given that Subcontractors all the way down the chain are obligated to comply with HIPAA even if their customers never ask them to sign a Business Associate Agreement. Service providers handling identifiable data (including information that may only contain dates of birth or zip codes) should consider seeking representations and warranties from all of their customers that such customers are not Business Associates under HIPAA. If a customer indicates that it is a Business Associate, the service provider must implement HIPAA-compliant controls with respect to the PHI.

If a company determines that it is a Subcontractor, it must comply with (i) the mandatory provisions applicable to Business Associates under HIPAA, including requirements to provide access, amendments, and accountings of disclosure with respect to PHI; (ii) the HITECH security breach notice obligations, which require notification of Breaches to the Business Associate; and (iii) the HIPAA Security Rule with respect to any ePHI created or received from or on behalf of a Business Associate. Note that these obligations include a requirement that a Subcontractor bind any subcontractor or third party with whom the Subcontractor shares PHI to the same restrictions as the Subcontractor. Therefore, Subcontractors must take care to include appropriate privacy and security language in their own agreements where they are sharing PHI with vendors and suppliers.

For more information about Final Rule, or about developments in privacy and security laws generally, please contact:

Jennifer J. Daniels (212) 885-5575 Daniels@BlankRome.com