Advisory

FEBRUARY 2013

If you have any questions about this Advisory, please contact:

MICHELLE WILCOX DEBARGE
860.297.3702
mdebarge@wiggin.com

JODY ERDFARB
203.363.7608
jerdfarb@wiggin.com

The Unusual Suspects: HIPAA's Applicability Broadly Expanded to Downstream Contractors

You've heard of HIPAA, but you've relegated it to something applicable only to health care companies. You've heard some of the recent hype about increasing penalties and aggressive enforcement, but you haven't paid much attention, happy knowing that HIPAA was something that you didn't have to worry about.

If this describes you, beware! Your organization may soon be required to comply with HIPAA, even if your connection to the health care industry is remote, requiring you to act fast to ensure compliance with this complex law.

BACKGROUND

Since its inception, HIPAA has been directly applicable only to covered entities, defined as health plans, health care clearinghouses, and health care providers that transmit health information in connection with certain standard claims-related electronic transactions. In 2009, however, Congress passed legislation known as the Health Information Technology for Economic and Clinical Health Act (HITECH), which amended HIPAA and extended the reach of some HIPAA obligations to certain contractors of covered entities, called "business associates."

On January 25, 2013, the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published new regulations, implementing HITECH's provisions and clarifying the scope and application of those requirements. As expected, the regulations apply many of HIPAA's requirements, including the HIPAA Security Rule, directly to business associates. *The regulations also expanded the definition of a business associate to include downstream contractors* that receive, access, maintain, or transmit protected health information on behalf of a business associate. Therefore, whereas previously the business associate obligations applied only to direct contractors of covered entities, now downstream contractors are potentially required to comply as well. *This regulatory change significantly broadens HIPAA's applicability, transforming the law from one that applied to a narrow category of covered entities and their business associates to one that potentially applies across a wide-range of downstream corporate entities.*

NEW LEGAL REQUIREMENTS

The new regulations require business associates and their subcontractors to comply with HIPAA's Security Rule, which contains 18 different administrative, technical, and physical security standards and over 30 implementation specifications. The Security Rule requires business associates and their subcontractors to conduct, and document, initial and ongoing risk assessments to evaluate their security controls against these standards and implementation specifications. The security controls must ensure the confidentiality, integrity, and availability of

CONTINUED ON NEXT PAGE

The Unusual Suspects: HIPAA's Applicability Broadly Expanded to Downstream Contractors CONTINUED

all electronic protected health information that the business associates and their subcontractors create, receive, maintain, or transmit; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and protect against any reasonably anticipated uses or disclosures of such information that are not permitted. While the Security Rule is based on the fundamental concepts of flexibility, scalability, and technology neutrality and no specific types of technology are required, organizations must consider and address in their assessments each security standard and implementation specification. These risk assessments are required regardless of the sophistication of the security system in place and must be updated on a periodic basis.

Also, the new HITECH regulations extend certain of the HIPAA Privacy Rule's use and disclosure and individual rights requirements to business associates and their subcontractors, such as the obligation to provide an accounting of disclosures of protected health information. The regulations also require business associates and their subcontractors to limit uses and disclosures of protected health information to the minimum necessary. Moreover, business associates and subcontractors will be required to provide the Secretary of HHS with access to their records to allow for an evaluation of their HIPAA compliance.

Finally, business associates and their subcontractors must ensure that they have in place compliant business associate agreements with covered entities and subcontractors, as applicable, and they also must amend their existing business associate agreements to ensure that they include new provisions mandated by the regulations. These new obligations will require organizations to draft and implement a multitude of HIPAA policies and procedures and to train their workforce accordingly.

DEADLINES

The new regulations become effective on March 26, 2013, but OCR provided an additional 180 days, until September 23, 2013, to become fully compliant. A business associate agreement that was compliant with the old regulations prior to January 25, 2013 and that is not renewed or modified between March 26, 2013 and September 23, 2013 does not have to be amended to comply with the new regulations until the earlier of: (1) the date that the agreement is renewed or modified after September 23, 2013 or (2) September 22, 2014.

ENFORCEMENT

Over the last several years, OCR has become increasingly aggressive in enforcing HIPAA compliance. Whereas enforcement used to be primarily complaint driven, OCR now proactively investigates and audits compliance; whereas OCR traditionally resolved investigations by merely requiring corrective action, it now imposes significant monetary penalties. This new trend of vigorous enforcement is due, in part, to OCR's increased resources and authority, pursuant to HITECH.

Prior to HITECH, OCR was prohibited from imposing civil monetary penalties in excess of $25,000 per calendar year for the same violation. HITECH increased this maximum penalty to $1.5 million and mandated that OCR audit covered entities and business associates for compliance. HITECH further provided the state Attorneys General with the authority to enforce HIPAA. OCR and the state Attorneys General have not been shy in wielding their new authority. OCR has imposed millions of dollars in fines since HITECH's passage and has rolled out a pilot audit program. State Attorneys General in several states have settled HIPAA cases for millions of dollars, including Connecticut, Vermont, Massachusetts, and Minnesota.

There is likely to be even more aggressive enforcement to come as collected monetary penalties are added to government coffers. Furthermore, HITECH requires the promulgation of regulations allowing individuals that are harmed by violations to receive a percentage of any collected civil monetary penalties. These regulations have not been published, but when they are, they most certainly will generate more complaint and enforcement activity triggered by financially motivated whistleblowers.

ACTION STEPS

If you are subject to HIPAA, it will take significant time and effort to become compliant, particularly if you have not yet implemented the HIPAA Security Rule, and you should take steps as soon as possible to comply.

As a first step, you should assess whether you are subject to the new requirements. The scope of the definition of business associates and subcontractors is potentially murky when applied in the context of real-world contractual relationships. Depending on the types of services and the level of access your workforce has to protected health information, whether you are a business associate or a subcontractor of

CONTINUED ON NEXT PAGE

The Unusual Suspects: HIPAA's Applicability Broadly Expanded to Downstream Contractors CONTINUED

a business associate may be very clear or it may be rather unclear. In any case, a careful and comprehensive analysis should be done to determine your status.

If you are required to comply with the new regulations, you will need to complete and document several inventories and assessments in connection with the protected health information you receive, access, maintain or transmit; develop and implement HIPAA-compliant policies and procedures; train your workforce; and enter into written agreements with covered entities and your own subcontractors, as applicable. Although these tasks will likely require considerable investment of time, effort, and financial resources, HIPAA compliance is legally required, and these expenditures may be relatively small in comparison to the potential penalties that OCR may impose for noncompliance.

As described above, these new regulations are merely the latest wave in the new era of increased HIPAA enforcement. As a business associate or subcontractor of a business associate, you need to be confident about your level of HIPAA compliance, be prepared for the possibility of an OCR audit or complaint investigation, and be able to defend your policies, procedures, and practices.

UPCOMING HIPAA PROGRAMS

Wiggin and Dana will be offering educational presentations on the changes to HIPAA. The presentations will take place from 8:30 - 11:30 a.m. on the following dates:

- Wednesday, February 27 - New Haven office
- Friday, March 1 - Hartford Hilton Hotel

Email rsvp@wiggin.com to register. Please indicate which location you would like to attend in the body of the email.