GOODWIN | PROCTER

March 12, 2009

Client Alert

An informational newsletter from Goodwin Procter LLP

Economic Stimulus Legislation Expands Scope and Enforcement of HIPAA

New Measure Makes Technology Company and Other Business Associates Independently Subject to HIPAA and Imposes Breach Notification Obligations Among Other Changes

On February 17, 2009, in response to concerns over continually weakening economic conditions, President Obama signed into law the American Recovery and Reinvestment Act of 2009 ("ARRA"). The ARRA has received a lot of attention for its tax and spending provisions. However, the legislation also makes very significant changes to certain aspects of healthcare regulation, in particular, the privacy and security of health information. Title XIII of ARRA, the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), dedicates $22 billion in federal funding to advance the use of health information technology. Recognizing that effective data privacy and security is a necessary prerequisite to the digitization of our healthcare system, Subtitle D of the HITECH Act also modifies dramatically the applicability of the security and privacy regulations that govern health-related information, as previously promulgated under the Health Insurance Portability and Accountability Act ("HIPAA"). Some of the most significant modifications are highlighted below.

Business Associates of HIPAA Covered Entities Are Now Independently Subject to HIPAA

The HITECH Act implements many noteworthy changes related to entities considered "business associates" under HIPAA. Most notably, the legislation makes business associates, and not just the covered entities to which they provide services, directly subject to HIPAA's privacy and security requirements as well as the penalties for violating those requirements. This expansion of the government's jurisdiction on HIPAA enforcement is a dramatic shift from former policy. Prior to the HITECH Act, business associates were not subject directly to HIPAA. Instead, HIPAA required the covered entity to contract with business associates to ensure that they would protect all protected health information ("PHI") obtained from the covered entity in accordance with HIPAA's requirements. As a result, prior to the HITECH Act, a business associate who failed to comply with HIPAA's security and/or privacy requirements would face only the threat of contractual liability with the covered entity with which it had entered into a business associate agreement, but not direct enforcement actions by regulators. Under the changes ushered in by the HITECH Act, business associates will now be subject to the same government civil and criminal penalties as covered entities.

Additionally, the HITECH Act subjects business associates to a number of the substantive provisions of the regulations, including the requirements to implement administrative, physical and technical safeguards, to protect PHI. Business associates must also now comply with the HIPAA regulation requiring the implementation of formal policies and procedures as well as documentation requirements. Business associates will need to review and revise existing privacy policies and practices.

Although the HITECH Act directly regulates the conduct of business associates, they are still required to enter into contractual agreements with covered entities. These contracts, whether new or already in existence, must reflect the aforementioned policy shift. Accordingly, covered entities and business associates will need to re-evaluate and revise existing business associate agreements. Additionally, any organization that transmits PHI to a covered entity or its business associate and requires routine access to such PHI, or any vendor that contracts with a covered entity to offer personal health records to patients as part of the covered entity's electronic health record, will be required to enter into a contractual agreement with the covered entity and will be treated as a business associate.

New Data Breach Notification Requirements

The HITECH Act also imposes new data breach notification requirements. While certain states (e.g. California, Arkansas) with breach notification laws have recently begun to extend the reach of those laws to breaches involving healthcare information, there has not been any federal requirement to date. Moreover, while the majority of states have breach notification laws for data that can be used to commit financial identity theft, only a small minority of states extend these requirements to health information.

Under the HITECH Act, covered entities will be required to notify individuals upon any compromise of their unsecured[1] PHI. Business associates will be required to notify covered entities of such a breach. The breach notification must be made without unreasonable delay and within no more than 60 days following the detection of the breach. Furthermore, if the breach involves the data of more than 500 individuals, the covered entity must notify the Department of Health and Human Services ("HHS") at the time of the discovery as well as "prominent media outlets" in the applicable area. Significantly, details of such large breaches will be posted on the HHS website for public viewing. With regard to breaches involving fewer than 500 individuals, in addition to the notification obligations, covered entities suffering a breach will be required to maintain a log of such breaches to be submitted annually to HHS.

The HITECH Act requires that HHS issue interim final regulations regarding these breach notification provisions no later than August 16, 2009. These new breach notification requirements will become effective 30 days after the date the interim final regulations are promulgated. The effective date should be no later than September 15, 2009, but will depend upon the date on which the final regulations are promulgated.

Expansion of Individual Rights

It is important to note that the HITECH Act also expands individual rights under the HIPAA Privacy Rule. Some of the most significant changes are new restrictions on selling of PHI, increased accounting rights and expansion of individual access rights.

Enforcement

The HITECH Act also expands enforcement and increases potential penalties. Some of the most significant changes are summarized below:

Audits

Prior to the new legislation, HHS was authorized to conduct audits of HIPAA privacy and security compliance. HHS is now required to conduct periodic audits in order to ensure compliance.

Investigations and Penalties

The HITECH Act also requires formal investigations into complaints of, as well as imposition of civil monetary penalties for, violations due to willful neglect. The HITECH Act amends the civil monetary penalty provisions for HIPAA violations to include tiered increases in the amounts of these penalties: (i) where a person "did not know" of the violation, a penalty of at least $100, but no more than $50,000, for each violation; (ii) where there was "reasonable cause" but no willful neglect, a penalty of at least $1,000, but no more than $50,000, for each violation; and (iii) where there was willful neglect, a penalty of at least $10,000, but no more than $50,000, for each violation. The total amount of penalties for all violations of an identical requirement or prohibition during a calendar year is capped in each tier. Significantly, the new civil monetary penalty provisions are effective and applicable immediately.

Attorney General Actions

The HITECH ACT authorizes, for the first time, individual state Attorneys General to bring civil actions against individuals who violate HIPAA privacy and security standards, in order to enjoin further violations and seek damages of up to $100 per violation, capped at $25,000 for all violations of an identical requirement or prohibition in a calendar year.

Effective Date

Most of the provisions of the HITECH ACT are to take effect February 17, 2010. Some provisions have an earlier effective date For example, as discussed above, the breach notification laws are expected to be effective no later than September 15, 2009. Moreover, and quite significantly, the increased civil penalties became effective upon enactment.

Implications

The HITECH Act includes important, new and far-reaching provisions concerning the privacy and security of PHI. The new requirements will a have material and direct impact on many organizations. The enactment of the HITECH Act constitutes the first federal breach notification requirement. Moreover, as has been discussed, the breach notification obligations are very broad. Accordingly, all companies, whether covered entities, business associates or other vendors, should be evaluating their existing breach notification policies and procedures and revising them to ensure compliance with the HITECH Act as well as any state law counterpart to the new federal breach notification provisions.

The changes ushered in by this new legislation will have a particular impact on business associates, as they mark a dramatic departure from and expansion of the legal obligations that had previously applied to such entities. Specifically, business associates should take steps now to determine whether they need to adopt HIPAA policies and update related materials that reflect their new status as directly subject to HIPAA. The law will also affect covered entities, who should be reviewing and revising existing privacy and security policies, administrative materials, record retention policies and training logs to ensure compliance with the new requirements. Of course, covered entities will also need to evaluate their existing relationships and agreements with their business associates and make all necessary modifications thereto.

---

[1] "Unsecured" PHI generally means information that is not encrypted or secured in such as manner as to make it unreadable to an unauthorized person. However, the Department of Health and Human Services is to issue guidance on the meaning of "unsecured" and other key terms.

If you would like additional information about the issues addressed in this Client Alert, please contact any of the attorneys listed below.

Deborah S. Birnbach	dbirnbach@goodwinprocter.com	617.570.1339
Louise N. Howe	lhowe@goodwinprocter.com	202.346.4139
Jacqueline Klosek	jklosek@goodwinprocter.com	212.459.7464

Full access to all articles prepared by Goodwin Procter is available here.