HUNTON& WILLIAMS

CLIENT ALERT

September 2009

Becoming HITECH: Actions Covered Entities and Business Associates Should Take Now to Comply with the Requirements of the HITECH Act

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Elizabeth H. Johnson
One Bank of America Plaza
Suite 1400
421 Fayetteville Street
Raleigh, NC 27601
(919) 899-3073
ehjohnson@hunton.com

Ryan P. Logan
One Bank of America Plaza
Suite 1400
421 Fayetteville Street
Raleigh, NC 27601
(919) 899-3085
rlogan@hunton.com

Additional Lawyers
Cédric Burton
Purdey Castle
Jörg Hladjk
Natalie Hunt
Christopher Kuner
Manuel E. Maisog
Melinda L. McLellan
Olivier Proust
Boris Segalis
Aaron P. Simpson
Rachel M. St. John
Bridget C. Treacy
Mason A. Weisz
John W. Woods, Jr.

Centre for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate

The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), which was signed into law in February 2009 as part of the economic stimulus package, substantially impacts requirements imposed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The HITECH Act creates several new and potentially burdensome obligations that affect the relationship between covered entities and business associates. Because these changes are quite substantial and necessitate revisions to existing business associate agreements ("BAAs"), covered entities and business associates should begin compliance efforts as soon as possible.

Application of the HIPAA Security Rule to Business Associates

Among the HITECH Act's provisions is a requirement obligating business associates to fully implement the information security safeguards specified by the HIPAA Security Rule. Implementation must be complete by February 17, 2010. Under current HIPAA regulations, business associates are not required to fully implement the Security Rule, but rather are required to implement safeguards that "reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic personal health information" that they create, receive, maintain or transmit on behalf of covered entities. As a result of the HITECH Act, however, business associates will need to implement written, comprehensive information security programs that address each aspect of the HIPAA Security Rule and covered entities will need to take steps to ensure their business associates' compliance.

The Security Rule details certain administrative, physical and technical safeguards, many of which must be documented. Examples of administrative safeguards include conducting periodic risk assessments regarding the vulnerability of electronic personal health information ("PHI") and designating an employee who is responsible for HIPAA security policies and procedures. Physical safeguards include facility access controls and device and media controls, including procedures for data backup, storage and final disposition of electronic PHI. Technical safeguards include role-based access controls and storage and transmission security such as encryption.

Although business associates may have implemented some of these safeguards, it is critical that they promptly conduct a rigorous evaluation of their information security policies, procedures and

practices to ensure that they have implemented a well-documented program that incorporates all of the requisite safeguards.

With respect to business associate contracting, covered entities also must take affirmative steps to address the expansion of the Security Rule. The HITECH Act requires covered entities to explicitly provide in their BAAs that all of the HITECH Act's security requirements applicable to covered entities are also applicable to business associates. BAAs also should be amended to reflect the HITECH Act's requirement that business associates must comply with the HIPAA Security Rule. Because it will likely take some time to negotiate new BAAs and conduct due diligence to establish that business associates have implemented the required safeguards, covered entities should begin both processes as soon as possible.

Breach Notification Provisions

The HITECH Act also imposes breach notification obligations that should cause covered entities to reevaluate their business associates and BAAs. Beginning on September 23, 2009, covered entities will be required to notify individuals of any breach of their "unsecured" PHI within 60 calendar days after the breach is discovered. The Department of Health and Human Services ("HHS") has stated, however, that it will not impose sanctions for failures to provide the required notifications for breaches that are discovered before February 22, 2010, but instead will "work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance." (For additional information on this point, please refer to the Hunton & Williams Privacy and Information Security Law Blog).

The 60-day breach notice deadline runs from the date a breach is discovered. The HITECH Act provides that a breach is "discovered" on the first day the breach is known, or should reasonably have been known, to have occurred by any employee, officer or agent of the covered entity. Establishing a discovery date based on the knowledge of any employee exacerbates the already-short 60-day deadline, and breach response activities (such as conducting forensic investigations, determining whether notice is legally required, and drafting notifications) are often quite time-consuming and raise complex legal issues. As a result, covered entities may wish to require in their BAAs that business associates notify them of any breach immediately or within a short, specified period, and require that notice must be provided in a specified manner to a specified contact point in order to maximize the time the covered entity will have to respond.

If a breach is discovered, business associates are required by the HITECH Act to notify covered entities and provide the identities of each affected individual. Covered entities are, in turn, required to notify affected individuals and, further, notify the Secretary of HHS if more than 500 individuals are affected. Prominent media outlets also must be notified in any state or jurisdiction where more than 500 individuals are impacted. For breaches affecting fewer than 500 individuals, covered entities must maintain a log of these breaches and submit it to HHS annually. As a result, significant attention may be paid to covered entities providing notice of a breach, emphasizing the need to appropriately manage business associates that handle PHI. Beyond simply modifying their BAAs, covered entities should engage in diligence to ensure that their business associates have implemented an effective incident response plan.

For business associates, the breach notification requirements necessitate evaluating their existing incident reporting mechanisms and, if they have not yet done so, implementing a robust information security program that enables them to detect and respond to information security breaches as quickly as possible. Such steps are necessary both to comply with the HITECH Act and to demonstrate to covered entity customers that they have effective response programs.

Accounting of Disclosures of PHI

Other provisions of the HITECH Act that will necessitate an evaluation of business associate relationships and contracting are the changes relevant to accountings of disclosures of PHI. The HIPAA Privacy Rule presently requires covered entities to maintain an accounting of certain disclosures of PHI for the prior six years, but carves out an exception for disclosures related to treatment, payment and health care operations. The HITECH Act, however, eliminates that exception for covered entities that use or maintain electronic health records ("EHRs") and entitles individuals to receive an accounting of treatment, payment and health care operation disclosures made in the prior three years. The HITECH Act further provides that, when an individual requests an accounting of such disclosures, a covered entity may respond by either: (1) providing the

requested accounting of all disclosures made both by the covered entity and by any business associates acting on its behalf; or (2) providing the requested accounting of all disclosures made by the covered entity and a list of all business associates acting on its behalf, at which point the individual may contact those business associates directly to request an accounting of disclosures made by them.

Covered entities will have to implement administrative and technical solutions to address their own accountings of disclosures, but also should consider the impact these changes have on their business associate relationships. Covered entities should, for example, revise their BAAs to require that business associates maintain such accountings and notify them of any requests for the same from individuals. Covered entities also should take steps to ensure that their business associates are capable of maintaining the requisite accountings and responding to any such requests. Business associates, in turn, should consider whether they need to implement administrative and technical solutions to enable them to produce and maintain an accounting of disclosures that will facilitate compliance with these enhanced requirements.

The provisions relating to accountings of disclosures become effective later than the other HITECH Act provisions discussed in this alert. For EHRs acquired on or before January 1, 2009, the provisions apply to disclosures made on or after January 1, 2014. For EHRs acquired after January 1, 2009, the provisions apply to disclosures made on or after the later of January 1, 2011 or the date the EHR was acquired.

We Can Help

Hunton & Williams' Privacy and Information Management practice has substantial experience preparing and advising on comprehensive privacy and information security programs (including those required by HIPAA), as well as vendor management programs. We also frequently assist clients in preparing for and responding to information security breaches. If you need assistance in developing, reviewing or implementing your organization's privacy or data security practices, please contact us.

Visit the Privacy and Information Security Law Blog at www.huntonprivacyblog.com for global privacy and information security law updates and analysis.