MAJOR HIPAA CHANGES AHEAD

The economic stimulus bill (the American Recovery and Reinvestment Act of 2009) signed into law on February 17, 2009 contained a series of stimulus measures relating to health information technology, including financial incentives for the adoption by health providers of electronic health record systems (the “HITECH Act”). A significant portion of the HITECH Act creates new HIPAA Privacy and Security Rules that will have major legal and operational consequences for health care providers. The summary below provides an overview of some of the more significant elements of the new requirements.

SECURITY BREACH NOTIFICATION REQUIREMENTS

Currently, HIPAA does not directly obligate Covered Entities to notify individuals of privacy or security breaches of their health information unless the Covered Entity determines that notification is necessary in order to mitigate damages. Under the HITECH Act, notification of breaches will be mandated in certain circumstances.

Notification must occur for any unauthorized acquisition, access, or disclosure of “unsecured protected health information” that compromises the privacy or security of such information, with some exceptions relating to the unintentional or inadvertent use or disclosure of such information by employees or other authorized individuals within an entity. These provisions apply to breaches involving both electronic and paper records. The United States Department of Health and Human Services (“HHS”) is directed to specifically define the term “unsecured protected health information” or “unsecured PHI” by April 17, 2009. A Business Associate (defined as a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a Covered Entity) must also notify a Covered Entity (as opposed to the affected individuals directly) of a breach of unsecured PHI.

The HITECH Act requires notification to individuals without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. Additionally, a Covered Entity must provide notice to HHS of all breaches that occur. If the breach involved 500 or more individuals, the notice to HHS must occur immediately and there will be a posting on the HHS public website. If the breach involves less than 500 individuals, a Covered Entity can maintain a log of breaches and submit the log to HHS annually. If the breach involves more than 500 residents of a state, then notice shall also be provided to prominent media outlets serving that state or jurisdiction.
HHS is required to issue interim final regulations to implement all of the breach notification requirements within 180 days after the enactment of the HITECH Act. The breach notification provisions become effective for breaches discovered 30 days after publication of the regulations.

BUSINESS ASSOCIATE OBLIGATIONS

One of the most significant changes to HIPAA is that the HITECH Act makes various provisions of the HIPAA Security and Privacy Rules directly applicable to Business Associates of Covered Entities in the same fashion as those provisions apply currently to Covered Entities. Under the HITECH Act, Business Associates will need to implement administrative, physical, and technical safeguards to comply with the Security Rules requirements; will need to designate a Security Officer; will need to implement a training program for workforce members regarding Security Rules compliance; and will need to conduct a security risk analysis.

A Business Associate is presently liable only for breaches of its obligations under the contractual provisions of its business associate agreement, and is not directly subject to HIPAA enforcement by the government. The new HITECH Act provisions now provide that HHS (as well as state attorneys general) may impose fines directly against Business Associates who do not comply with applicable HIPAA requirements.

Additionally, Business Associates will now be required to take steps to stop HIPAA violations of which they become aware when doing business with Covered Entities. A Business Associate may have to terminate a business associate agreement if it becomes aware of a pattern of activity or practice by a Covered Entity that violates the business associate agreement. If termination is not feasible, the Business Associate may be required to report the Covered Entity’s compliance problem to HHS. These new requirements will also need to be added to existing business associate agreements and they will likely increase the cost and risks involved with being a Business Associate. These new requirements are effective on or about February 17, 2010.

ENHANCED ENFORCEMENT PROVISIONS

The new HITECH Act substantially increases the governmental enforcement of the existing HIPAA regulations by: (1) increasing the civil monetary penalties and civil settlement amounts; (2) adding provisions on willful neglect violations; and (3) allowing state attorneys general to enforce any HIPAA violations.

Under the HITECH Act, there will now be a new tiered system in which a civil monetary penalty is linked to the level of intent of the violator. If the violator of the HIPAA regulations did not know of the violation, the range of penalties is from a minimum of $100 per violation to $25,000 for violations of the same requirement in a calendar year. Violations resulting from “reasonable cause” but not “willful neglect” can result in penalties of $1,000 per violation and up to $100,000 for violations of the same requirement in a calendar year. In both cases, the maximum range of civil monetary penalties is $50,000 per violation, but no more than $1,500,000 for violations of the same requirement in a calendar year.
For violations committed with willful neglect, if the neglect is corrected within 30 days from when the violator knew or should have known of the violation, the range of penalties is a minimum of $10,000 per violation, but no more than $250,000 for violations of the same requirements in a calendar year and a maximum of $50,000 per violation but no more than $1,500,000 for violations of the same requirement in a calendar year. If the willful neglect violation remains uncorrected, the minimum violation is $50,000 per violation with no set maximum penalty.

Most of the penalty levels and requirements detailed above are effective immediately. Also, very significantly, HHS is now also tasked to develop a regulation by February 17, 2012 which will permit the distribution of a portion of the civil monetary penalty proceeds directly to harmed individuals. This will likely incentivize individuals to report alleged HIPAA violations to HHS as well as to state attorneys general, who will also be able to commence state actions.

Under the HITECH Act, individuals (including employees of Covered Entities) who are not themselves Covered Entities may violate HIPAA and be subject to penalties if PHI is maintained by a Covered Entity and the employee or other individual obtained or disclosed the PHI without authorization.

HHS is also now authorized to audit both Covered Entities and Business Associates to ensure compliance with the HIPAA regulations.

ADDITIONAL PROVISIONS

The HITECH Act also amended several additional HIPAA provisions, including the following:

- HHS must issue, within the next 18 months (by August 17, 2010), specific revised guidance on the definition of “minimum necessary.” Until the new guidance is issued, Covered Entities and Business Associates are directed to limit disclosures to a “limited data set” to the extent practicable or to the minimum necessary to accomplish the intended purpose.

- The accounting requirement has been changed such that a Covered Entity must now account for all disclosures of PHI used or maintained in an electronic health record related to payment, treatment and health care operations for a period of three years. New regulations will be issued as to what specific information must be included in this accounting. The effective date of these changes for current (prior to January 1, 2009) users of electronic health records is January 1, 2014. For entities acquiring an electronic health record system after January 1, 2009, the effective date is January 1, 2011 or the date the system is acquired, whichever is later.

- Covered Entities may not sell electronic health records or PHI obtained from an electronic health record without a valid authorization except in very limited circumstances. HHS is required to issue regulations regarding this change within 18 months after enactment of the HITECH Act and the provisions become effective six months later.
An individual has the right to obtain a copy of information in an electronic format from any Covered Entity that uses or maintains an electronic health record with respect to PHI of that individual. A Covered Entity may not impose a fee that exceeds the labor costs for providing this information. This requirement is effective on or about February 17, 2010.

The rules now further restrict the use of PHI for marketing purposes. In particular, a communication by a Covered Entity or Business Associate about a product or service that encourages recipients to purchase or use that product or service is not a health care operation (and therefore requires an individual’s authorization) except under limited circumstances. Also, a Covered Entity may not receive direct or indirect remuneration in exchange for communications except in limited circumstances. This requirement is effective on or about February 17, 2010.

The HITECH Act mandates that Covered Entities comply with requests from individuals that their PHI not be disclosed to a health plan if the purpose for the disclosure is for payment or health care operations (and is not related to treatment) and the health care services to which the PHI applies have been paid for out-of-pocket in full. This requirement is effective on or about February 17, 2010.

The HITECH Act requires fundraising opt-out provisions to be “clear and conspicuous.” Also, the HITECH ACT requires that Covered Entities treat any opt-out as a revocation of an authorization. This requirement is effective on or about February 17, 2010.

Please note that this summary is not an exhaustive discussion regarding the changes to HIPAA, but rather is intended to provide an overview of important elements of the new regulations. If you have any questions regarding these new regulations, please do not hesitate to contact any member of our firm’s Health Care Group at (585) 232-6500.