Fox Rothschild LLP
ATTORNEYS AT LAW

FEBRUARY 2009

HEALTH LAW PRACTICE
ALERT

HITECH Act Greatly Expands Scope of HIPAA's Applicability and Enforcement and Increases Civil Monetary Penalties for Violations

By Michael Kline

Those who are superstitious may believe that bad things happen on Friday the 13th, but we will leave it to each individual and entity to formulate conclusions regarding the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), which Congress passed late on Friday, February 13, 2009, and President Obama officially signed into effect on February 17, 2009.

The HITECH Act addresses various aspects relating to the use of health information technology (H.I.T.), including providing for federal funding by way of grants and incentive payments in order to promote H.I.T. implementation. This *Alert* focuses, however, on Subtitle D of the HITECH Act, which includes important, new and far-reaching provisions concerning the privacy and security of health information that will materially and directly affect more entities, businesses and individuals in more diverse ways than ever before. These changes are further elaborated upon below, but this *Alert* can only highlight certain prominent issues under the HITECH Act and is by no means a comprehensive review of this lengthy and complex Act. For questions and additional guidance on the HITECH Act, contact your Fox Rothschild attorney or the authors of this *Alert*.

Civil Monetary Penalties and Enforcement Expanded

The HITECH Act amends the civil monetary penalty (CMP) provisions for HIPAA violations to include tiered increases in amounts of CMPs as follows:

- Where a person "did not know," at least $100, but no more than $50,000, for each such violation
- Where there was "reasonable cause" but no willful neglect, at least $100, but no more than $50,000, for each such violation
- If there was willful neglect, at least $10,000, but no more than $50,000, for each such violation

The new CMP provisions are effective and applicable immediately to all violations occurring from and after the date of enactment of the HITECH Act. Also, within three years after the enactment of the HITECH Act (February 17, 2012), the Secretary of the federal Department of Health and Human Services (DHHS) is obligated to establish regulations that will allow individuals harmed by privacy and security violations to receive a percentage of any CMP or monetary settlement collected with respect to such offense.

The HITECH Act also authorizes each state attorney general (AG) for the first time to begin pursuing civil actions for HIPAA privacy and security violations that have threatened or adversely affected a resident of the AG's respective state. For any violation that occurs on or after February 17, 2009, state AGs are now authorized to obtain **statutory damages** on

behalf of any such residents of their state in an amount equal to $100 for each violation of a single requirement, up to a total of $25,000 for violations of that requirement. Attorneys' fees are also allowed to be collected by an AG for pursuing civil actions for HIPAA privacy and security violations.

Expanded Applicability

The HITECH Act now **directly** obligates business associates to comply with the HIPAA Security Rule's administrative, physical and technical safeguard requirements, including developing and implementing comprehensive written security policies and procedures with respect to the protected health information (PHI) that they handle. Failure by business associates to abide by such requirements can result in CMPs being assessed *directly* against them.

In addition, any organization, with respect to a covered entity, that provides data transmission of PHI to such entity (or its business associate) and that requires access to PHI on a routine basis must now be treated as a business associate and enter into a HIPAA-compliant business associate agreement. Examples of such entities include Health Information Exchange Organizations, Regional Health Information Organizations, or **"any vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record."** Where such entities would now be considered "business associates," they then are also required to directly comply with the HIPAA Security Rule provisions, which the HITECH Act made directly applicable to business associates. It then follows that such organizations are now also directly subject to potential CMPs and statutory damages for violations.

New Privacy and Security Requirements

- **Security Breach Notification Requirements:** Security breach notification requirements under the HITECH Act go into effect 30 days after the date that interim final regulations are promulgated, which will be no later than 180 days after the date of enactment of the HITECH Act (August 16, 2009). Covered entities, business associates and vendors who handle personal health records are required to abide by breach notification requirements. Violations of this requirement by vendors would be treated as an unfair and deceptive act or practice in violation of the Federal Trade Commission Act. If a breach affects more than 500 individuals of a particular state, notice also must be provided to prominent media outlets following the discovery of the breach.
- **Complying with Requested Restrictions:** Every covered entity must now comply with an individual's requested restriction on how it uses and discloses the individual's PHI if the disclosure is to a health plan for purposes of carrying out payment or health care operations, and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.
- **Minimum Necessary Disclosures:** Within 18 months after the date of enactment of the HITECH Act (August 17, 2010), new guidance shall be issued governing what constitutes the "minimum necessary" for purposes of disclosures under the privacy rule. Covered entities must, when otherwise permitted, disclose only the "minimum necessary" to accomplish the intended purpose for such disclosure.
- **Accounting of Disclosures with EHRs:** Covered entities that use and disclose PHI through electronic health records (EHRs) are required to provide individuals with an accounting, when requested, for the prior three-year period. Uses and disclosures of PHI through EHRs include treatment, payment and health care operations. Covered entities with EHRs may need to begin accounting for disclosures as early as January 1, 2011, depending on when they acquire and begin to use an EHR.
- **Access Rights to Electronic Format:** The HIPAA Privacy Rule is amended to give individuals the right to obtain access to their PHI in electronic format, if they so request.
- **Health Care Operations:** The definition of "health care operations" will be reviewed by the Secretary of DHHS by August 17, 2010, and narrowed or clarified.
- **Marketing:** The HIPAA Privacy Rule is amended to limit when a covered entity may

disclose PHI as part of a health care operation if it receives or has received direct or indirect payment in exchange for making such communication, except in specified circumstances.

- **"Sale" of PHI:** Covered entities and business associates are prohibited from directly or indirectly receiving any *remuneration* in exchange for any PHI of an individual unless a valid authorization is obtained from the individual, except in a very limited number of circumstances, including research, public health activities, treatment of the individual, and in connection with the sale of a covered entity to a buyer of the business. The narrow list of exceptions are all subject to any additional restrictions that may be found in regulations regarding "sale of PHI" to be promulgated by the Secretary of DHHS no later than August 17, 2010. The effective date of the ban on the sale of PHI under the HITECH Act is six months after the date that the final regulations are promulgated.
- **Effective Date:** Unless otherwise specified, the effective date of all provisions is one year from the date of enactment of the HITECH Act, or **February 17, 2010**.

What Should Affected Entities Do?

At a minimum, affected entities that are already subject to HIPAA compliance should begin making the following changes:

- Update Notice of Privacy Practices to reflect changes in privacy and security policies
- Update HIPAA privacy and security policies accordingly
- Develop a detailed Breach Notification Policy that complies with HITECH and any state law counterpart to the new federal breach notification provisions
- Expand business associate lists to include vendors and others
- Update Business Associate Agreements to include expanded new requirements

What Should Entities that Have Not Previously Been Subject to HIPAA Do?

Entities that have not yet been subject to HIPAA compliance or have had limited compliance requirements under HIPAA should examine the new scope of HIPAA, as it may be applicable to them under the HITECH Act in order not to unintentionally become non-compliant.

For more information about this *Alert*, contact Michael Kline at 609.895.6635 or mkline@foxrothschild.com.
Visit us on the web at www.foxrothschild.com.

Fox Rothschild LLP
ATTORNEYS AT LAW

Attorney Advertisement