porterwright

Health Care and Information Privacy Law Alert

A Corporate Department Publication

March 2009

This Health Care and Information Privacy Law Alert is intended to provide general information for clients or interested individuals and should not be relied upon as legal advice. Please consult an attorney for specific advice regarding your particular situation.

Ann M. Caresani
216-443-2570
acaresani@porterwright.com

Theodore G. Fisher
614-227-2040
tfisher@porterwright.com

Brian D. Hall
614-227-2287
bhall@porterwright.com

Richard J. Helmreich
614-227-2088
rhelmreich@porterwright.com

Robert J. Morgan
614-227-2186
rmorgan@porterwright.com

James H. Prior
614-227-2008
jprior@porterwright.com

Donna M. Ruscitti
614-227-2192
druscitti@porterwright.com

Richard G. Terapak
614-227-4301
rterapak@porterwright.com

Jeremy A. Logsdon
614-227-2093
jlogsdon@porterwright.com

Kenneth K. Rathburn
614-227-2128
krathburn@porterwright.com

Please see our other publications at www.porterwright.com/publications.

HITECH Act Brings New Vigor to HIPAA's Privacy and Security Rules

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA). Title XIII of ARRA, the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), significantly changes the landscape of federal privacy and security law as it relates to protected health information (PHI).

The HITECH Act, among other things, (i) creates new data breach notification requirements for breaches of unsecured PHI, (ii) expands the list of entities considered to be business associates (Business Associates) under the HIPAA Privacy and Security Rule and for the first time makes Business Associates directly subject to these Rules, (iii) modifies the Privacy Rule in several respects, and (iv) strengthens the enforcement provisions of HIPAA.

Notifications of Data Breach

The HITECH Act's data breach notification requirements apply to covered entities, such as health plans, health care providers, and health care clearing houses (Covered Entities) and, to a lesser extent, to Business Associates. The notification requirements are similar to those contained in data breach laws that have been enacted in a majority of states. Most of the state data breach laws, however, specifically exempt Covered Entities from any notification or disclosure obligations. Under the HITECH Act, Covered Entities, many of which may be unfamiliar or unaware of typical state data breach notice requirements, must now prepare themselves to respond — quickly and properly — to a data breach event.

Under the HITECH Act, a data breach notification requirement is triggered when a Covered Entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise uses unsecured PHI (UPHI) knows or reasonably should have known that UPHI has been accessed, acquired, or disclosed as a result of a "breach." A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security of such information. Upon triggering the data breach notification requirement, Covered Entities must follow specific content, timing, and method requirements as outlined in the HITECH Act:

- Timing: All notices must be made within 60 days from when the Covered Entity becomes aware of the breach (subject to law enforcement requests to delay such notice).

- Content: All notices must include (i) a brief description of the breach, including the date of breach and discovery; (ii) a description of the types of UPHI disclosed or misappropriated during the breach; (iii) the steps individuals can take to protect their identity; (iv) a description of the Covered Entity's actions to investigate the breach and mitigate harm now and in the future; and (v) contact procedures (including a toll-free telephone number) for affected individuals to find additional information.
- Method: All Covered Entities must notify affected individuals in writing by first class mail (unless the individuals have opted for electronic communication with the Covered Entity). If the Covered Entity has insufficient contacts with the individuals, an alternative notice method (posting on website, broadcast media, etc.) may be permitted.

The HITECH Act includes two additional mandatory notice requirements and one discretionary notice. First, the Covered Entity must immediately notify the Secretary of Health and Human Services if a breach affects more than 500 individuals, after which the Secretary will post the Covered Entity's name on its internet website. For breaches involving fewer than 500 individuals, the Covered Entity may maintain a log of such breaches to submit annually to the Secretary. Second, the Covered Entity must publish a notice in a prominent media outlet in each state or jurisdiction in which more than 500 individuals' UPHI has been breached. Finally, a Covered Entity may give telephonic notice to individuals if the Covered Entity reasonably believes there is a possibility of imminent misuse of UPHI; however, such telephonic notice will not substitute for a Covered Entity's written notice obligations.

Additionally, the HITECH Act states that the Secretary shall provide guidance (no later than 60 days after enactment) as to the definition of UPHI. If no such guidance is given, UPHI shall mean PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization accredited by the American National Standards Institute.

The HITECH Act also imposes notification requirements upon Business Associates. Business Associates who discover a breach of unsecured PHI must notify the Covered Entity of such breach, including in such notice the identity of each individual whose unsecured PHI is believed to have been accessed, acquired or disclosed.

Expanded Definition, and Direct Regulation, of Business Associates under Privacy and Security Rules

The HITECH Act also broadens the definition of Business Associate to encompass "vendors" of personal health records (PHR) and "third-party service providers" to such vendors. The HITECH Act provides that each PHR vendor, following the discovery of a breach of security of unsecured PHR (UPHR), must notify each individual whose UPHR was acquired by an unauthorized person as a result of the breach. The vendor or third-party service provider must also notify the Federal Trade Commission. Data breach notification requirements that are applicable to Covered Entities, such as timing, method, and content, also apply to vendor notifications.

Importantly, effective one year from the date of enactment, the HITECH Act also makes all Business Associates subject to various provisions of the Privacy Rule and Security Rule that previously were reserved for Covered Entities only. Until now, the obligations of Business Associates regarding PHI were governed by private contract law, pursuant to the terms and conditions of a business associate agreement with a Covered Entity. The HITECH Act now makes Business Associates subject to the Security Rule's requirements regarding administrative, physical and technical safeguards and its policies, procedures and documentation requirements, as well as any additional security requirements added by the HITECH Act. With respect to the Privacy Rule, the HITECH Act codifies the use and disclosure restrictions that previously applied to Business Associates only by contract and makes Business Associates subject to any additional privacy requirements added by the Act. To the extent the HITECH Act imposes any new privacy or security requirements, these must be incorporated in business associate agreements between a Business Associate and a Covered Entity.

Modifications to HIPAA Privacy Rule

The HITECH Act also modifies the Privacy Rule in several respects, including with respect to accounting of disclosures of PHI made through an electronic health record (EHR), patient consent for disclosures of PHI for marketing purposes, individual requests for restriction on disclosures of PHI, access to PHI in electronic format, and prohibitions against sale of EHRs or PHI.

Accounting of Disclosures made through EHRs; Access to PHI in Electronic Format

Under HIPAA's current disclosure rules, a patient may request an accounting of all disclosures of their PHI over the previous six-year period, subject to certain exceptions, such as disclosures for purposes of payment, health care

operations, or treatment. The HITECH Act modifies HIPAA's Privacy Rule such that the accounting of disclosures made through an EHR must include all disclosures for purposes of payment, health care operations, or treatment over the past three years. For EHRs acquired before January 1, 2009, the new accounting requirements apply to all disclosures for purposes of payment, health care operations, or treatment occurring on or after January 1, 2014. If an EHR is acquired after January 1, 2009, however, the new accounting requirements apply to all such disclosures occurring on or after January 1, 2011. Covered Entities that maintain patient records in EHRs must allow patients to access their PHI in electronic form.

Patient Consent for Disclosures of PHI for Marketing Purposes; Prohibitions Against Sale of EHRs or PHI

Currently, HIPAA's Privacy Rule requires that a Covered Entity obtain patient consent for disclosure of PHI for "marketing purposes," unless the disclosure meets an exception or is considered part of "health care operations." Under the HITECH Act, a Covered Entity may only classify a disclosure as part of "health care operations" if it meets a specific marketing exception. Also, the HITECH Act prohibits a Covered Entity from receiving any remuneration for the disclosure absent prior patient consent. This prohibition is subject to certain exceptions. With certain enumerated exceptions, the HITECH Act also prohibits the sale of an individual's PHI without a valid authorization from the individual. HHS must issue regulations regarding this prohibition within 18 months.

Individual Requests for Restrictions on Disclosures of PHI

HIPAA's Privacy Rule currently allows patients to request that the Covered Entity restrict the use or disclosure of their PHI, even for purposes of payment, health care operations, or treatment, but the Covered Entity may refuse to agree to such a request. Under the HITECH Act, a Covered Entity must honor the request if the disclosure is to a health plan for purposes of carrying out treatment, payment or health care operations and the PHI relates solely to treatment or services for which the health care provider has been paid out-of-pocket and in full. This restriction likely would require Covered Entities to link their accounts receivable and patient treatment functions in order to know when such non-disclosure requests must be honored.

Strengthened Enforcement Provisions

The HITECH Act strengthens HIPAA's enforcement provisions. Among other things, in addition to potential criminal penalties, the HITECH Act increases civil penalty amounts ranging from a minimum of $100 per violation where a person did not know (and by exercising due diligence would not have known) of a violation to a maximum of $50,000 per violation (with a cap of $1,500,000 for violations of an identical requirement during a calendar year) where the violation is due to willful neglect. Also, in a move that has the potential to significantly increase enforcement activity, the HITECH Act authorizes state attorneys general to bring civil actions in federal court to enjoin violations of HIPAA or to seek damages on behalf of individuals.

Conclusion

The HITECH Act significantly increases the responsibilities of Covered Entities and Business Associates in dealing with PHI. Both Covered Entities and Business Associates must review current practices and procedures immediately and seek assistance where necessary to achieve compliance with the requirements of the Act.