



WHAT HEALTH CARE ENTITIES NEED TO KNOW ABOUT HIPAA AND THE AMERICAN RECOVERY AND REINVESTMENT ACT

by Lane W. Staines and Cheri D. Green

On February 17, 2009, The American Recovery and Reinvestment Act of 2009 (“ARRA”) was signed into law, greatly expanding the existing federal regulations on health information technology. Title XIII of the ARRA includes the Health Information Technology for Economic and Clinical Health Act, also known as the HITECH Act. The HITECH Act increases the enforcement of penalties for violations of HIPAA, mandates compliance with new notification policies for breaches of protected health information (“PHI”), and perhaps most significantly, requires Business Associates to comply with HIPAA Privacy and Security Rules.

The changes under HIPAA and the HITECH Act are expansive and pervasive. This summary is only a thumbnail sketch of the significant changes. As rules and regulations are interpreted, modified and further elaborated upon, you will need to continue to monitor the changing landscape.

APPLICATION OF PRIVACY AND SECURITY RULE TO BUSINESS ASSOCIATES

A Business Associate is an individual or corporate “person” that performs on behalf of the Covered Entity any function or activity involving the use or disclosure of protected health information and is not a member of the Covered Entity’s workforce. Prior to the enactment of the ARRA, the HIPAA Privacy and Security Rules applied only to Covered Entities, and business entities indirectly complied with these Rules through their contracts, often known as Business Associate agreements, with Covered Entities. If a Business Associate violated its obligations under the Privacy and Security Rules, such violations were treated as contractual breaches.

Under the HITECH Act, a Business Associate who accesses PHI pursuant to a written contract with a Covered Entity is subject to the same civil and criminal penalties under HIPAA



as the Covered Entity. Business Associates will be required to be in full compliance with HIPAA and must implement administrative safeguards for the protection of electronic protected health information (“ePHI”) (45 C.F.R. § 164.308), physical safeguards to limit physical access to ePHI (45 C.F.R. § 164.310), and technical safeguards for electronic information systems that control access to ePHI (45 C.F.R. § 164.312). Additionally, Business Associates must implement policies and procedures to comply with all other requirements of the HIPAA Security Rule and must provide documentation of security safeguards (45 C.F.R. § 164.316). A business entity’s failure to meet these requirements will be treated the same as such a failure by the Covered Entity.

Business Associates must also meet requirements of the HIPAA Privacy Rule under the HITECH Act. Specifically, Business Associates must only use PHI as necessary under its Business Associate agreement and as authorized by 45 C.F.R. § 164.504(e). As with the Security Rule, a Business Associate’s violation of the Privacy Rule may result in civil and/or criminal penalties.

As a result of these changes, Covered Entities need to amend their Business Associate agreements to reflect these heightened security and privacy requirements and take steps to educate their Business Associates on these changes under the HITECH Act. Most provisions under the Security and Privacy rules have a compliance date of February 17, 2010.

IMPACT OF BREACH NOTIFICATION PROVISIONS ON COVERED ENTITIES AND BUSINESS ASSOCIATES

A breach is the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security, privacy, or integrity of PHI. Prior to the enactment of the HITECH Act, Covered Entities were not required to inform patients, or HHS, of privacy or security breaches of PHI. However, under Section 13402 of the Act, Covered Entities are now required to notify individuals whose unsecured PHI has been accessed or disclosed as a result of a breach, and Business Associates are required to notify a Covered Entity of such a breach. Unsecured PHI is PHI that is not secured through the use of a technology or methodology specified by HHS. HHS will issue guidance by May 16, 2009 as to the appropriate “technology or methodology” that should be used to encrypt, or otherwise secure, PHI from unauthorized individuals, and further guidance on breach notification provisions will be provided by August 16, 2009.



Notice of a breach must be given to the individual, or next of kin if deceased, in writing via first-class mail to the last known address “without unreasonable delay” and no later than 60 days after discovery of the breach. If the individual has expressed a preference to be contacted by electronic mail, notification by such is permitted. When contact information is insufficient or out-of-date, substitute notice may be made. The notice must briefly describe what happened, the date of the occurrence, the date of discovery, the type of information breached, the steps individuals should take to protect themselves, a brief description of the investigation and mitigation process, and contact information.

If ten or more individuals’ information is breached and there is insufficient information for all, the Covered Entity must provide notice through a posting on the entity’s website or in a major print or broadcast media with a toll-free contact telephone number. If the PHI of more than 500 individuals in a State is believed to have been breached, notice must be provided to “prominent media outlets” in the area. Typically, the Secretary of HHS must be given notice of breaches annually, but if the PHI of more than 500 individuals has been breached, notice must be provided immediately.

DISCLOSURES OF PROTECTED HEALTH INFORMATION

Accounting of Disclosures

HIPAA grants patients the right to receive an accounting of certain disclosures of their PHI for the six-year period prior to the request. However, Covered Entities have not been required to account for disclosures of PHI made for treatment, payment or health care operations. Under Section 13405(c) of the HITECH Act, Covered Entities must now account for disclosures of PHI for these purposes for the three years prior to the request for an accounting. Although the time frame is now only three years, this new provision will require health care entities to reevaluate their electronic health record (“EHR”) technology to ensure that each disclosure is duly noted for its particular purpose. An electronic health record is an electronic record of an individual’s health information that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Covered Entities that did not have an EHR as of January 1, 2009, must comply with this provision by the later of January 1, 2011, or the date on which the entity acquires an EHR. Covered Entities that did have an EHR as of January 1, 2009, are given a more distant deadline, January 1, 2014, for compliance.



Patients' Access to PHI: Under the HITECH Act, individuals are given the right to obtain a copy of their PHI in electronic format, if the Covered Entity uses an EHR.

Restrictions on Disclosures: Although Covered Entities were previously allowed to deny individuals' requests for restrictions on disclosures of their PHI for treatment, payment or health care operations, section 13405(a) of the HITECH Act now requires Covered Entities to grant requests for restrictions if the disclosures are to health plans to carry out payment or health care operations and the PHI pertains to a service for which the patient paid the healthcare provider in full out-of-pocket.

"Minimum Necessary": HIPAA requires hospitals and health care entities to ensure that the disclosure of PHI is only the "minimum necessary" needed for the requested purpose. The HITECH Act requires the HHS to issue guidance as to the specific meaning of "minimum necessary" under the Privacy Rule by August 17, 2010. Until this clarification, the "minimum necessary" requirement is satisfied only if a Covered Entity or Business Associate uses a "limited data set" which excludes identifiers like names, street or postal address information, telephone numbers, etc. If the PHI cannot be limited to a "limited data set," Covered Entities and Business Associates must determine what constitutes the "minimum necessary" and disclose only that information.

Marketing

The HITECH Act limits the current exceptions to the definition of "marketing" in 45 C.F.R. § 164.501(1) so that a communication is considered marketing if the Covered Entity receives direct or indirect remuneration for it unless the communication (1) describes a drug or biologic that is prescribed for the recipient of the communication and payment received by the Covered Entity for such communication is reasonable; (2) is made by the Covered Entity who has obtained authorization from the recipient of the communication; or (3) is made by a Business Associate on the Covered Entity's behalf pursuant to a contract between the two.

A Covered Entity or Business Associate can no longer receive remuneration for disclosure of PHI unless the individual has signed an authorization which acknowledges that remuneration will be paid. Certain exceptions, such as disclosures for public health, research, and payments by an individual for a copy of his or her records, apply.



Fundraising

The HITECH Act simply makes the requirement that Covered Entities provide an opportunity for individuals to opt out of fundraising communications a statutory, rather than regulatory, provision.

Enforcement

Criminal Penalties

Although only Covered Entities previously could be held directly liable for violations of HIPAA, individuals may now be held criminally liable for obtaining or disclosing, without authorization, identifiable health information that is maintained by a Covered Entity.

Civil Penalties

The HITECH Act enacts many changes to previous enforcement provisions under HIPAA. Under section 13410(a) of the Act, HHS is required to investigate any complaint that may have resulted from “willful neglect” by a Covered Entity or Business Associate.

Additionally, the Act includes a provision for victims of privacy violations to receive a share of penalties that are collected after the necessary compensation methodology is completed by the anticipated February 17, 2012 deadline. Further, Section 13410(d) establishes civil monetary penalties ranging from \$100 per violation to up to \$50,000 per violation, depending on the nature, extent and harm of the violation. Where a person did not know, and by exercising due diligence still would not have known, of a violation, the minimum penalty is \$100 per violation with a cap of \$25,000 for violations of the same requirement during a calendar year, and the maximum penalty is \$50,000 per violation with a cap of \$1.5 million for violations of the same requirement during a calendar year. If a violation is due to “reasonable cause,” the minimum penalty is \$1,000 per violation, capped at \$100,000 total for violations of an identical requirement, and the maximum penalty is \$50,000, capped at \$1.5 million. Where a violation is due to “willful neglect,” the penalties range from \$10,000 to \$50,000 per violation and up to \$250,000 to \$1.5 million for all violations of an identical requirement during a calendar year.

If the Secretary has not already instituted an action, state attorneys are authorized to bring civil actions against violators of the Privacy and Security Rules to enjoin such violations or to obtain damages on behalf of state residents for the violations. In such cases, actions are limited to \$100 per violation but not to exceed \$25,000.



Audits

The Secretary must conduct periodic audits to confirm that Covered Entities and Business Associates are in compliance with the HIPAA Privacy and Security Rules.

For any questions about the HITECH Act or assistance in implementing these changes, please contact Cheri Green at (601) 960-6864 or cgreen@brunini.com or Lane Staines at (601) 973-8755 or lstaines@brunini.com or other members of Brunini's Health Care Law Group.