The HITECH Act: An Overview of Its Impact on Business Associates

Kathryn H. Rowan[1]

The Health and Information Technology for Economic & Clinical Health Act ("HITECH"), signed into law on February 17, 2009, was enacted as part of the American Recovery & Reinvestment Act of 2009 ("ARRA") to strengthen the HIPAA Security Rule by imposing civil money penalties that the Department of Health and Human Services could enforce for violations of the HIPAA Rules. These amendments to HIPAA's enforcement regulations address privacy and security concerns associated with the electronic transmission of health information and will have a significant impact on attorneys and law firms and their healthcare clients.

Privacy & Security of Personal Health Information

In 1996, HIPAA was passed and assigned the responsibility to promulgate and enforce regulations to the Department of Health and Human Services ("HHS"). In 2001, HIPAA's Privacy Rule became effective and provided guidance on the appropriate uses and disclosures of protected health information. HIPAA's later Security Rule, adopted in 2003, established policies and procedures for securing protected health information.

The adoption of the HITECH Act expands the current federal privacy and security protections for health information. As described in a paper by the Majority Staff of the Committees on Energy and Commerce, Ways and Means, and Science and Technology (January 16, 2009), the legislation accomplishes this by:

- Establishing a federal breach notification requirement for health information that is not encrypted or otherwise made indecipherable. It requires that an individual be notified if there is an unauthorized disclosure or use of their health information.
- Ensuring that new entities that were not contemplated when the federal privacy rules were written, as well as those entities that do work on behalf of

providers and insurers, are subject to the same privacy and security rules as providers and health insurers.

- Providing transparency to patients by allowing them to request an audit trail showing all disclosures of their health information made through an electronic record.
- Shutting down the secondary market that has emerged around the sale and mining of patient health information by prohibiting the sale of an individual's health information without their authorization.
- Requiring that providers attain authorization from a patient in order to use their health information for marketing and fundraising activities.
- Strengthening enforcement of federal privacy and security laws by increasing penalties for violations and providing greater resources for enforcement and oversight activities.

Business Associates

The changes will have a significant impact not only Covered Entities, but also on Business Associates. Attorneys and law firms who serve as Business Associates for their healthcare clients and receive or access their clients' protected health information are now statutorily required to comply with HITECH and are directly subjected to the HIPAA safeguards.

While there are several pertinent effective dates under HITECH, one of the more significant effective dates was February 17, 2010 when the application of the rules to, and accountability for, Business Associates became effective. The HITECH Act extends certain conditions of HIPAA's civil and criminal penalties to Business Associates, who are now directly required to comply with the safeguards contained in the HIPAA Security Rule. Previously, Business Associates were subjected to HIPAA privacy and security requirements only via contractual agreements with Covered Entities. The HITECH Act now places Business Associates under the same comprehensive Security Rule requirements as Covered Entities to ensure consistency of security when health information is accessed or exchanged between organizations.

The HITECH Act §13400(2) states that "Business Associate" has the meaning given to that term in 45 C.F.R., §160.103, which states:

> "A Business Associate is a person who on behalf of a Covered Entity or organized healthcare agreement but "[p]rovides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person."

Some examples of Business Associates include third party billing companies, transcriptionists, data storage companies, IT companies, data shredding companies, and attorneys providing legal service to a health plan which involves access to personal health information. Basically any entity that is exposed to or works with the protected health information on behalf of a Covered Entity would qualify as a Business Associate.

New Requirements for Business Associates

Part I, §13401 of the HITECH Act applies the HIPAA Administrative Safeguards (§164.308), Physical Safeguards (§164.310), Technical Safeguards (§164.312) and Policies and Procedures and documentation requirements (§164.316) to Business Associates of Covered Entities in "the same manner that such sections apply to the Covered Entity." These security requirements must also be incorporated into Business Associate agreements between Business Associates and their Covered Entities.

Breach Notice Requirements

Business Associates are now required to report a breach of unsecured protected health information to the associated Covered Entity, providing the identification of "each individual whose unsecured protected health information has been, or is reasonably believed by the

Business Associate to have been, accessed, acquired, or disclosed during such breach."[2] The Covered Entity is then required to notify each affected individual. If a breach involves 500 patients or more, then the Covered Entity must notify HHS. If a breach involves "more than 500 residents of such State or jurisdiction" notice shall be provided to prominent media outlets serving the State or jurisdiction.[3]

Content of the notice must including the following: 1) a brief description of what happened, the date of breach, and the date the breach was discovered; 2) a description of the types of unsecured protected health information involved in the breach; 3) precautionary steps individuals should take to protect themselves from the "potential harm resulting from the breach"; 4) a description of the investigation of the breach by the Covered Entity; and 5) contact procedures for affected individuals to follow to obtain additional information.[4]

Enforcement

Under Subtitle D, §13400 of the HITECH Act, there are four levels of violations. Each level reflects an increasing level of culpability to which "Covered Entities" and "Business Associates" now may be subject to civil and criminal penalties:

- The first tier involves violations that are unknown and by *exercising reasonable diligence* would not have been known. Penalties range from $100 for each violation, with the total amount for all such violations in a calendar year not to exceed $25,000.

- The second tier involves violations due to *reasonable cause* and not to *willful neglect*. The penalties for each violation range from $1,000 for each violation, with the total amount for all such violations in a calendar year not to exceed $100,000.[5]
- The third tier involves violations of provisions due to *willful neglect if corrected* within 30 days from knowledge of the violation. The penalties range from $10,000 for each violation, with the total amount in a calendar year not to exceed $250,000.

- The fourth tier involves violations of *willful neglect that are uncorrected*. The penalties range from $50,000 for each violation, with the total amount for all such violations in a calendar year not to exceed $1,500,000.

As with HIPAA, an individual cannot bring a cause of action against a provider under the HITECH Act. However, it does allow for a state attorney general to bring an action on behalf of residents of the state.

Many Affirmative Defenses No Longer Available

§13410(d) removes the affirmative defense for violations in which the Covered Entity did not know or by reasonable diligence would not have known of the violation. Such violations are now subject to the first tier of penalties.

The Act also amended the subsection that provides an affirmative defense for a 30 day time period of correction to only require that the Covered Entity demonstrate the violation *was not due to willful neglect*:

> "A Covered Entity that did not know and reasonably should not have known of such violations, will not have this affirmative defense available *unless* it also corrects the violation during the 30 day time period beginning on the first date of such knowledge or during the period determined appropriate by the Secretary based on the nature and extent of the failure to comply."[6]

The statute on its face suggests that the knowledge involved must be knowledge that a violation has occurred, not just knowledge of the facts constituting the violation. Furthermore, this defense is not available in the event a covered entity's "lack of knowledge" resulted from its failure to inform itself about its compliance obligations or investigate received complaints or other information indicating likely noncompliance.[7]

Conclusion

As of January 1, 2011, Covered Entities and Business Associates are now required to provide, upon request, an accounting of disclosures of protected health information if the

Covered Entity uses an electronic health record. Clearly, the HITECH will continue to impose additional requirements on Covered Entities and now Business Associates, such as audits and accounting of disclosures, with the ultimate goal of electronic health records by 2014.

Business Associates are now squarely in the middle of the HIPAA and HITECH world through the electronic exchange of protected health information, as they will now be held directly liable for breaches of protected health information. If they have not done so already, Business Associates should (1) review their HIPAA policies and procedures to ensure compliance with the Security Rule safeguards and (2) review their Business Associate agreements with Covered Entities to ensure that the new requirements are incorporated.

---

[1] Kathryn Rowan is an Associate, Christian & Small LLP. Her practice focuses on insurance regulatory, compliance, and coverage matters, ERISA and employee benefits law and complex litigation.

[2] 45 C.F.R. § 13402, Notification In the Case of Breach.

[3] 45 C.F.R. § 13402(e)(2), Methods of Notice.

[4] 45 C.F.R. § 13402(f), Content of Notification.

[5] Reasonable cause is defined under §160.401, as "circumstances that would make it unreasonable for the Covered Entity despite the exercise of ordinary business care and prudence to comply with the administrative simplification provision violated."

[6] *See* Summary of 45 C.F.R. Part 160, Federal Register, Vol. 74, No.209, Oct. 30, 2009.

[7] *See* Summary of 45 C.F.R. Part 160, Federal Register, Vol. 74, No.209, Oct. 30, 2009.