

HITECH IN A HIGH TECH ERA

Abby Pendleton, Esq.
Jessica L. Gustafson, Esq.¹
The Health Law Partners, P.C.
Southfield, MI

The Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), included as part of the American Recovery and Reinvestment Act of 2009 (“ARRA”), significantly alters and supplements provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) protecting the privacy and security of individuals’ protected health information (“PHI”). Subtitle D of HITECH—pertaining to patients’ privacy rights, breach notification, and consequences of breaching private information—significantly expands the HIPAA privacy and security provisions. This article will summarize some key aspects of the privacy and security portions of the HITECH Act.

LIABILITIES OF COVERED ENTITIES AND BUSINESS ASSOCIATES

In one of the most significant expansions of HIPAA effectuated by the HITECH Act, the HITECH Act expanded certain requirements, which previously only governed covered entities,¹ to also govern business associates of covered entities.² Specifically, Section 13401 of the HITECH Act directly applied the administrative, physical and technical safeguard requirements of the HIPAA Security Rule to business associates, and mandated that business associates maintain policies, procedures and documentation of security practices. In addition, pursuant to Section 13404 of the HITECH Act, the privacy requirements



addressed by the HITECH Act (and summarized in this article) are made applicable not only to covered entities, but also to their business associates.

Whereas HIPAA specifically governed covered entities, and thus made only covered entities liable for HIPAA violations, *both covered entities and business associates are liable for HIPAA violations based on the HIPAA amendments in the HITECH Act.* Prior to HITECH, it was the covered entity’s responsibility to ensure the business associate complied with HIPAA standards. If a business associate committed a HIPAA violation, the consequence was termination of the contract if the business associate remained non-compliant. Now, if a business associate is non-compliant, then that business entity is subject to consequences directly from the HHS, including criminal and civil liabilities.

REQUIRED NOTIFICATION FOR INFORMATION BREACHES

Effective September 23, 2009, *both covered entities and their business*

*associates will be liable for breaches of a patient’s unsecured protected health information.*³ The HITECH Act requires a covered entity or its business associate to notify an individual of a breach of that individual’s unsecured protected health information within 60 days of discovering the breach. When a breach involves individual consumers, depending on the number of individuals who are involved, an individual notification or media notification will be utilized. Notification must also be made to the Department of HHS immediately if the breach involves 500 or more individuals. If the breach involves less than 500 individuals, the provider can maintain such information on a log, which must be provided annually to HHS.

Guidance from HHS Surrounding Breach Notification

On April 29, 2009, HHS published additional guidance regarding the HITECH Act’s requirements regarding the breach notification requirements for unsecured protected health information.⁴ Note that the breach notification requirements apply only to *unsecured* protected health information, which is defined as protected health information that is not unusable, unreadable or indecipherable to unauthorized individuals.

The additional guidance was mandated by Section 1302 (h) (2)

Continued on page 26

¹ A covered entity is defined as “(1) [a] health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.”

² A business associate is “a person or organization, other than a member of a covered entity’s workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review and billing.” <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>

³ Unsecured protected health information is defined as “protected health information that is not secured through the use of a technology or methodology specified by the Secretary....” HITECH § 13402(h)(1)(A).

HITECH IN A HIGH TECH ERA

Continued from page 25

of the HITECH Act, which required HHS to issue guidance “specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals” Although compliance with this guidance is not mandatory, HHS emphasized that following the guidance will serve as a safe harbor, resulting in “covered entities and business associates not being required to provide the notification otherwise required by section 13402 in the event of a breach.”

On August 24, 2009, HHS published an Interim Final Rule,⁵ which clarifies guidance specifying technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals, and further outlines new regulations governing covered entities’ and business associates’ responsibilities under the HITECH Act to provide notification to affected individuals and to HHS following the discovery of a breach of unsecured PHI. The new regulations will be codified at 45 C.F.R. § 164.400 *et seq.*

THE STAKES ARE RAISED – INCREASED ENFORCEMENT

As noted above, the HITECH Act contains provisions so that penalties that apply to covered entities for violations of HIPAA also apply to business associates. Further, the HITECH Act revises and expands current penalty provisions for violations of health privacy and security regulations. The HITECH Act contains new provisions related to noncompliance due to “willful neglect” and requires the government to formally investigate any complaint of a violation if a preliminary investigation of the facts indicates a possible violation due to willful neglect. The HITECH Act also replaces the



current penalty of \$100 per violation with a new tiered-penalty system.

Of particular importance, the HITECH Act also includes a provision authorizing enforcement by State Attorney General Offices if the attorney general of a State has reason to believe that an interest of one or more residents of that State has been or is threatened or adversely affected. In such cases, the Attorney General can bring a civil action on behalf of the state residents to enjoin any continuing violation or to obtain damages on behalf of the residents. The court may also award costs and reasonable attorney fees to the State.⁶

REQUIRED ACCOUNTING OF DISCLOSURES INVOLVING ELECTRONIC HEALTH RECORDS

As many providers are aware, under HIPAA, covered entities are not required to provide individuals with an accounting of disclosures of their protected health information if the disclosure is related to treatment, payment, or the health care operations of the covered entity. Per the HITECH Act, providers who use or maintain electronic health records will be required to account for disclosures related to treatment, payment, or the health care operations of the covered entity. In such cases, the accounting period is limited to three (3) years prior to the date on which the accounting is requested. The effective date for this new requirement is dependent upon whether the provider acquired an electronic health records as of January 1, 2009 or after January 1, 2009. For users of electronic records

⁴ 74 Fed. Reg. 19006 (April 17, 2009), available at <http://edocket.access.gpo.gov/2009/pdf/E9-9512.pdf>

⁵ 74 Fed. Reg. 42740 (August 24, 2009), available at <http://frwebgate6.access.gpo.gov/cgi-bin/PDFgate.cgi?WAISdocID=282472267445+0+2+0&WAIAction=retrieve>

⁶ Section 13410 of the HITECH Act.

as of January 1, 2009, the HITECH Act applies to disclosures made on and after January 1, 2014. For users acquiring electronic health records after January 1, 2009, the HITECH Act applies to disclosures made on and after the later of January 1, 2011 or the date the entities acquires the electronic health record.⁷

THE MINIMUM NECESSARY RULE

With regard to non-treatment situations, HIPAA requires providers to only use the minimum amount of PHI necessary to accomplish permitted tasks. Section 13405 of the HITECH Act clarifies that a covered entity will be seen as having complied with this “minimum necessary” standard if it limits the disclosed PHI to the “limited data set.” The limited data set excludes identifying information such as names, addresses, telephone numbers, social security numbers, etc. However, if the limited data set is not sufficient, the minimum necessary standard applies. By August 2010, HHS will issue guidance surrounding the definition of minimum necessary. Until this guidance is issued, the Act requires “in the case of the disclosure of protected health information, the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.”

PROHIBITIONS ON SALE OF ELECTRONIC HEALTH RECORDS OR PHI

Unless one of six (6) specified exceptions apply, the HITECH Act prohibits a covered entity or business associate from directly or indirectly receiving remuneration in exchange for any protected health information, unless the entity obtained a valid HIPAA authorization that specifies whether the

protected health information can be further exchanged for remuneration. The exceptions to the general prohibition include the following:

- The purpose of the exchange is for public health activities;
- The purpose is for research and the price charged reflects the costs of preparation and transmittal of the data for such purpose;
- The purpose is for treatment, subject to additional protections promulgated by regulation;
- The purpose is in connection with the business operations of the entity;
- The purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement;
- The purpose of the exchange is to provide an individual with a copy of his or her own protected health information.


HHS is authorized to develop additional exceptions. Notably, the effective date for this provision is six (6) months after the date of the promulgation of final regulations (HHS is responsible for promulgating regulations no later than 18 months after the enactment date of the Act).⁸

ACCESS TO INFORMATION IN ELECTRONIC FORMAT

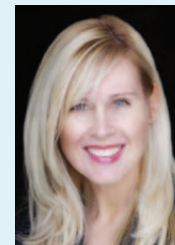
The HITECH Act states that where a covered entity uses or maintains an electronic health record with respect to protected health information, the

individual shall have a right to obtain from the covered entity a copy of such information in an electronic format.⁹

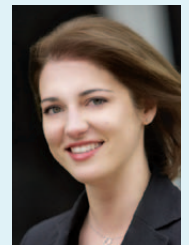
CONCLUSION

The HITECH Act significantly alters and supplements provisions of HIPAA protecting the privacy and security of individual’s PHI. Providers and their business associates are well advised to familiarize themselves with such requirements in order to remain in compliance with the expanded health information privacy and security requirements. 

ⁱ The authors would like to thank Neda Mirafzali, a 3L law student at Michigan State University Law School and a law clerk currently working with The Health Law Partners, P.C., for her contributions to and assistance with this article.



Abby Pendleton



Jessica L. Gustafson

Abby Pendleton and Jessica L. Gustafson are partners with the health care law firm of The Health Law Partners, P.C. The firm represents hospitals, physicians, and other health care providers and suppliers with respect to their health care legal needs. Pendleton and Gustafson co-lead the firm’s Recovery Audit Contractor (“RAC”) and Medicare practice group, and specialize in a number of areas, including: RAC, Medicare, Medicaid and other payor audit appeals, healthcare regulatory matters, compliance matters, reimbursement and contracting matters, transactional and corporate matters, and licensing, staff privilege and payor de-participation matters. Pendleton and Gustafson also regularly assist attorneys with their health care legal needs. They can be reached at (248) 996-8510 or apendleton@thehlp.com and jgustafson@thehlp.com.

⁷ Section 13405 (c) of the HITECH Act.

⁸ Section 13405 (d) of the HITECH Act.

⁹ Section 13405 (e) of the HITECH Act.