HIPAA Goes HITECH

By Laura Jeanne Sanger, M.S., J.D., C.I.P., LL.M. Candidate (Health Law)
ljsanger@gmail.com

On February 13, 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), as part of President Obama's stimulus package (The American Recovery and Reinvestment Act of 2009). The HITECH Act made important changes to the Health Insurance Portability and Accountability Act (HIPAA), particularly with regards to privacy provisions. Part of the HITECH Act is entitled "Improved Privacy Provisions and Security Provisions."

Enacted in part to assist healthcare providers who are, or will be, utilizing electronic health records (EHR) systems, the HITECH Act addresses consumer access to their EHR, increases application of HIPAA privacy standards to business associates of covered entities, and implements a tiered system of civil monetary penalties for HIPAA violations. Generally, the provisions of the HITECH Act are scheduled to become effective on February 17, 2010, the anniversary of President Obama signing the Act into law. This paper highlights some of the changes to HIPAA as modified by the HITECH Act; it is not an all-inclusive list, and individuals with specific questions should seek legal counsel.

Background

The Hippocratic Oath discussed maintaining the confidentiality of information acquired in the physician-patient relationship:

> "[w]hatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private."[1]

In order to protect information from wrongful dissemination by healthcare providers, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[2] An important part of HIPPA, known as the Privacy Rule, was developed to address the electronic transfer of private patient information.[3]

The Privacy Rule seeks to prevent dissemination of protected health information (PHI), i.e., that sort of information that a patient might have an expectation will not be shared without his or her permission. Enumerated in 45 C.F.R. § 164.514,[4] an individual's PHI

[1] Nat. Lib. of Med. and Nat. Inst. of Health, *The Hippocratic Oath*, http://www.nlm.nih.gov/hmd/greek/greek_oath.html.
[2] U.S. Dep't of Health & Human Servs., *Summary of the HIPAA Privacy Rule*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited July 22, 2009).
[3] *Id.*
[4] 45 C.F.R. § 164.514 (2009); *see also* 45 C.F.R. § 164.514(2)(i). Other requirements relating to uses and disclosures of protected health information. The following identifiers of an individual or of relatives,

includes information that could identify and/or reveal medical information about the person.

The HITECH Act: Business Associates

Prior to the passage of the HITECH ACT, covered entities[5] – such as health plans and health care providers – were required to fully comply with the standards and requirements of HIPAA. Business associates of covered entities were not directly regulated. Business associates are external businesses (as in they are not part of the covered entity) that provide services for, or to, the covered entity using protected health information (PHI) of an individual.[6] Business associates and covered entities have contractual agreements which govern the business associate's handling of PHI.

Under the HITECH Act, business associates are now responsible for complying with the provisions and regulations of HIPAA[7] and are directly answerable to the government for HIPAA breaches. Business associates are now also directly liable for civil and criminal penalties.[8] This increased statutory liability for business associates under HIPAA will likely result in the necessity of updating business associate and vendor lists as well as re-negotiating business associate agreements. In addition, business associates will most likely incur costs associated with bringing themselves into direct HIPAA compliance. The Secretary of the Department of Health and Human Services (HHS) will ultimately issue guidance regarding these safeguards.[9]

---

employers, or household members of the individual, are removed: (A) Names; (B). All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and any other unique indentifying number, characteristic, or code, except as permitted by paragraph (c) of this section;…

[5] 45 C.F.R. § 164.103. Covered entity means: "(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."

[6] *Id.*

[7] Pub. L. No. 111-05, H.R. 1, 111th Cong. (2009) (enacted in Title IV).

[8] Pub. L. No. 111-05, H.R. 1, 111th Cong. (2009) (enacted in Title XIII of HITECH Act, Sub. D, Sec. 13401(b)). In the case of a business associate that violates any security provision specified in subsection (a), Sections 1176 and 1177 of the Social Security Act (42 U.S.C. §§ 1320d-5, 1320d-6) shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision.")

[9] *Id.* at § 13401(c).

Breach Notification

The HITECH Act also expands the notification requirements due to breaches of an individual's PHI. Both covered entities[10] and business associates[11] are now obligated to notify individuals of breaches of their PHI. In cases where more than 500 "residents of [a] State or jurisdiction" have had their PHI breached, "prominent media outlets" serving that area must also be notified.[12] Individuals should be notified in writing, or e-mail if that is their preferred method of contact,[13] and be provided with basic information about the breach, such as:

- when the breach happened, when the event was discovered, and a brief statement about what happened;
- what type of PHI was breached;
- things that the individual can do in order "to protect themselves from potential harm resulting from the breach";
- what corrective actions and investigation the covered entity is doing to prevent future breaches and mitigate losses; and
- contact information for the individual to use in case of any questions.[14]

Reports to the Secretary of HHS describing any breaches are required to be made at least annually (where fewer than 500 breaches are reported) and immediately where more than 500 breaches of PHI are reported.[15]

Restrictions on Certain Disclosures and Sales of Health Information

The HITECH Act additionally outlines restrictions on the sale and disclosure of an individual's PHI. A significant change is a provision allowing individuals a right to have an accounting of all electronic heath record disclosures made using their PHI over the last three years from the date of the initial request.[16]

Also, the selling[17] of electronic health records and PHI, unless there is authorization to do so from the individual, is prohibited by this section.[18] There are seven exceptions to this prohibition, however:

(A) The purpose of the exchange is for public health activities...;

[10] *Id.* at § 13402(a).
[11] *Id.* at § 13402(b).
[12] *Id.* at § 13402(e)(2).
[13] *Id.* at § 13402(e)(1)(A).
[14] *Id.* at § 13402(f).
[15] *Id.* at § 13402(3).
[16] *Id.* at § 13405(c)(B). ("An individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested.")
[17] Id. at § 13405(d)(1) ("a covered entity or business associate shall not directly or indirectly receive remuneration").
[18] *Id.* at § 13405(d).

(B) The purpose of the exchange is for research … and the price charged reflects the costs of preparation and transmittal of the data for such purpose;
(C) The purpose of the exchange is for the treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent protected health information from inappropriate access, use, or disclosure;
(D) The purpose of the exchange is [for specific] health care operations;
(E) 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;
(F) The purpose of the exchange is to provide an individual with a copy of the individual's protected health information…;
(G) The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate [in keeping with other] exceptions…[19]

In addition to disclosure accounting, the individual is also entitled to receive a copy of his or her electronic health record, if they request; this information may be sent to the individual, or another person designated by individual.[20]

Guidance on "Minimally Necessary"

One way to prevent personal information from being lost is to never collect it in the first place. This concept is articulated as the "minimum necessary" standard: only the information necessary to achieve clinical and/or research goals should be gathered.[21] Defining and implementing this standard, particularly with regards to disclosure of PHI, is left to the determination of covered entities and their business associates.[22] Under the HITECH Act, the Secretary of HHS is directed to issue guidance on the "minimum necessary" standard, taking into account "the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease."[23]

Tiered Increases in Amount of Civil Monetary Penalties[24]

The HITECH act provides a tiered architecture of civil monetary penalties for HIPAA violations. This system is designed around the level of cognizance with regards to the violation – the lowest penalties are assigned where there was no knowledge of the violation, and the highest where there was an element of "willful neglect." The tiered

[19] *Id.* at § 13405(d)(2).
[20] *Id.* at § 13405(e).
[21] 45 CFR § 164.502(b).
[22] Pub. L. No. 111-05, H.R. 1, 111th Cong. (2009) (enacted in Title XIII of HITECH Act, Sub. D, Sec. 13405(b)(2)).
[23] *Id.* at § 13405(b)(1)(B).
[24] *Id.* at § 13402(d).

system takes into account the harm done by the violation, as well as the nature and extent of the violation.[25] In summary, the tiered system provides for:

Paragraph (Sec. 13410(d)	Violation Tier	Per Violation Penalty	Total amount imposed per person, per year, "for all such violations of an identical requirements of prohibition" maximum
(3) (A)	"did not know/would not have known"; at least (3)(A), not to exceed (3)(D)	$100	$25,000
(3) (B)	"reasonable cause" in the violation; at least (3)(B), not to exceed (3)(D)	$1000	$100,000
(3) (C)	"willful neglect," with corrective actions; at least (3)(C), not to exceed (3)(D)	$10,000	$250,000
(3) (D)	"willful neglect," violation not corrected; at least (3) (D)	$50,000	$1,500,000

Another important change provided by the HITECH Act is that state attorneys general may now bring civil lawsuits, in a *parens patriae* capacity, on behalf of state citizens for HIPAA violations.[26] This is in addition to the abilities of state attorneys general to bring actions under state statues[27] on behalf of the state against the person committing the violation.[28] If a federal action regarding the same issue is pending, the state action may not be brought at the same time.[29]

Additionally, some states' laws governing unauthorized use of identifying information can be quite stringent. In Texas, for example, chapter 48 of the Texas Business and Commerce Code provides that the unauthorized use of identifying information imposes a liability of $2,000 to $50,000 *per violation*, with no cap on total damages.[30]

Summary

HIPAA has been criticized for simultaneously failing to provide adequate protection of PHI, and for failing to provide mechanisms that would allow sufficient access to data to promote beneficial medical research.[31] With the creation of a national electronic medical records system, a specific health care reform goal of the Obama Administration, the scope and efficiency of HIPAA is being reevaluated.[32]

To a certain extent, the operations of regional health information organizations (RHIOs) can be referenced when contemplating modifications to HIPAA.[33] While RHIOs may

[25] *Id.* at § 13410(d)(C)(ii).
[26] *Id.* at § 13410(e).
[27] *Id.* at § 13410(e)(5).
[28] *See* TEX. BUS. & COMM. CODE ANN. § 48.201(b) (Vernon 2009).
[29] Pub. L. No. 111-05, H.R. 1, 111th Cong. (2009) (enacted in Title XIII of HITECH Act, Sub. D, Sec. 13410(e)(7)).
[30] TEX. BUS. & COMM. CODE ANN. § 48.201 (Vernon 2009).
[31] L.O. Gostin and S. Nass, *Reforming the HIPAA Privacy Rule: Safeguarding Privacy and Promoting Research*, 301:13 JAMA 1373-75 (2009).
[32] *Id.*
[33] C. McDonald, *Protecting Patients in Health Information Exchange: A Defense of the HIPPA Privacy Rule*, 28:2 HEALTH AFFAIRS 447-49 (2009).

serve as exemplars of low risk/high need medical records systems (as opposed to national databases that may be classified as high-risk/low need), allowing patient control over the transfer of information within the system may alleviate some of the security concerns with EHR.[34] The provision of notification of patients regarding access to their medical information may assist in developing systems that both alert and apprise patients of PHI access, while allowing visibility for research opportunities.

In teaching the enumerated HIPAA classifications of identifying information,[35] this author occasionally refers to the list as "information you would not want your stalker to know." While perhaps a bit dramatic, it brings home the point that these categories of information are the type that many individuals want to have control over, and would prefer to know to whom and why this information is being conveyed. Misuse of this information can range from traditional forms of identity theft (e.g. acquiring credit cards) to more sophisticated fraud schemes involving Medicare/Medicaid claims. In addition, information might be stigmatizing or potentially deleterious to the interests of the patient/subject, as in medical information regarding sexual history, drug abuse,[36] or mental health status. Information should be safeguarded with an eye towards HIPAA's traditional notion of collecting only "minimally necessary" information and safeguarding it if acquired.

Health Law Perspectives (August 2009)
Health Law & Policy Institute
University of Houston Law Center
http://www.law.uh.edu/healthlaw/perspectives/homepage.asp

[34] *Id.*
[35] *See* 45 C.F.R. § 164.514(2)(i).
[36] *See* 42 C.F.R. pt. 2 (Confidentiality of Alcohol and Drug Abuse Patient Records).