By Michael S. Khoury and Amy K. Fehn

# *Changes to HIPAA Privacy and Security Resulting from the HITECH Act*

## Introduction

HIPAA, the Health Insurance Portability and Protection Act, imposes obligations on all persons who deal with personal health information ("PHI") to protect the security and privacy of that information. Covered entities under HIPAA are generally health care providers that create or use PHI, as well as health care plans and health care clearinghouses. The Health Information Technology for Economic and Clinical Health Act ("the HITECH Act")[1] was enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA")[2] on February 17, 2009. The HITECH act, in addition to creating monetary incentives for the adoption of Electronic Health Record technologies ("EHRs"), contains several provisions that are intended to strengthen the HIPAA Privacy and Security Rules. Most revisions are effective on February 17, 2010.

## Increased Penalties and Enforcement

Perhaps the most talked about aspect of the revisions contained in the HITECH Act is the increased focus on enforcement and penalties. Penalties will be tiered based on the knowledge of the violation, with penalties of up to $50,000 per violation and up to $1,500,000 for identical violations imposed for offenses rising to the level of "willful neglect."[3] Importantly, the revised law requires governmental audits of covered entities rather than the current complaint-based system of enforcement. Increased penalties and required audits are effective immediately.

The HITECH Act also authorizes state attorneys general to immediately bring civil actions to enforce an individual's rights and to recover attorney fees from covered entities including damages.[4] The HITECH Act also requires the Secretary of Health & Human Services ("HHS") to establish, within three years, regulations that will allow harmed individuals to recover a portion of penalties assessed against a covered entity.[5]

### *Direct Liability for Business Associates*

Another significant change is that business associates will be directly responsible for complying with the same HIPAA privacy and security safeguards as HIPAA covered entities, including the new breach notification provisions.[6] Business associates include entities or people who provide services to a covered entity that requires the utilization of protected health information and can include transcription companies, consultants, attorneys, answering services, and billing services. The government will be allowed to bring penalties and fines against business associates for breaches in the same manner they are brought against covered entities. Previously a business associate's only liability under HIPAA was its contractual liability to the covered entity.

### *Breach Notification Requirements*

HITECH also brings in breach notification obligations that the financial industry and businesses have already addressed for other personal information.[7] The new HITECH requirement requires notification to patients, the government, and sometimes the media in the event of a privacy or security breach. Currently, if a breach occurs, the covered entity's only duty from a HIPAA standpoint is to "mitigate harm," which does not always necessitate notifying individuals. The new revisions make it mandatory to notify individuals within sixty days of discovery of a breach, and, depending on the number of people involved and the availability of contact information, could require media notifications. Providers will also be required to maintain a log of breaches and report them to the HHS annually.

The Office of Civil Rights (OCR) for HHS recently released guidance and a request for public comment on the HITECH act breach notification provisions.[8] The guidance discusses covered entities' notification obligations in the event of the unauthorized disclosure of "unsecured" protected health information. "Unsecured protected health information" is defined as protected health information that is *not* secured by technology standards that make it unusable, unreadable, or indecipherable to unauthorized persons and is developed and endorsed by a standards developing organization that is accredited by the American National Standards Institute (ANSI).

The guidance also discusses examples of methodologies that can be used to secure protected health information, including a discussion of valid encryption processes and destruction processes. This guidance and the breach notification requirements will go into effect thirty days after the issuance of interim final regulations, which are expected in mid-August. Thus, the effective date for the notification provisions is expected to be mid-September 2009.

The notification requirements will require covered entities and business associates of covered entities to revise their policies and will also require modification of business associate agreements to reflect the new obligations.

### *Accounting of Disclosure Requirements*

Another significant change is found in the HIPAA Privacy Rule's "accounting of disclosures" requirements. Currently, providers are not required to track or account for disclosures made for purposes of treatment, payment, and health care operations. The revisions to the rule will remove this exception for providers who utilize an electronic health record.[9] More details on the exact format and content of

information that must be reported to patients on request will be set forth in future regulations. The effective date of this provision varies based on how long the covered entity has utilized an EHR. Covered entities that have adopted an EHR as of January 2009 are given the most time and have until January 2014 to become compliant with this requirement.

### *Closure of Marketing "Loophole"*

The revisions to the HIPPA Privacy Rule also eliminate what some privacy advocates perceive as a marketing "loophole." The current rule allows certain treatment recommendations without an authorization. The revised rule continues to allow such communications but prohibits providers from receiving any compensation in return, subject to very limited exceptions.[10]

### *Right to Copy of Electronic Health Record*

Health care providers who utilize an EHR will be required to provide an electronic copy to a patient, on request of the patient, subject only to the cost of labor incurred in responding to the request.[11] Interestingly, the format of the electronic copy is not specified. This may lead to issues in the future, as some EHRs may not have the capability to produce an electronic copy that is readable by commonly used software.

### *Right to Restrictions of Certain Disclosures to Health Plans*

A covered entity must comply with an individual's request that information not be disclosed to a health plan, if the disclosure is not for the purpose of treatment and the services at issue have already been paid in full out of pocket.[12]

### *Prohibition on the Sale of PHI*

The HITECH Act contains a prohibition on the sale of protected health information through an EHR or otherwise, subject to certain limited exceptions or the individual's specific authorization. The Secretary of HHS is required to issue regulations to carry out this provision within eighteen months of the implementation date of the HITECH Act.[13]

### *More Specific Guidance*

The revised law also contains several provisions that require more specific guidance on varying aspects of the HIPAA Privacy and Security Rules. Currently, the HIPAA Security Rule is "technologically neutral," which creates considerable confusion among providers, attorneys, and consultants when trying to determine exactly what needs to be done, especially where small providers are concerned. The HITECH Act requires the Secretary of HHS to issue annual guidance on the most effective and appropriate technical safeguards. The "minimum necessary" requirements will also be clarified through more specific guidance, which is required to be issued within eighteen months of the enactment date of the HITECH Act.[14]

### *New Business Associate Categories*

The HITECH Act also requires organizations that provide data transmission of protected health information and require routine access to protected health information to enter into business associate agreements with the covered entities that offer the protected health information.[15]

## Conclusion

The HITECH Act increases both security and privacy responsibilities of everyone dealing with PHI. This follows the trend of increased regulation and protection of personal information. Future regulations are expected to clarify and provide guidance on many of these provisions. Attorneys who counsel covered entities and business associates of covered entities should stay apprised of future developments and should review client policies and procedures to ensure that they are in compliance with new requirements.

**NOTES**

1. 42 USC 300jj et seq. (Pub L No 111-5, 123 Stat 226) (2009).
2. Pub L No 111-5, 123 Stat 115 (2009).
3. 42 USC 1320d-5(5)(a)(3).
4. 42 USC 1320d-5(d).
5. 42 USC 13410(c)(3).
6. *See* 42 USC 17934.
7. 42 USC 17932.
8. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf.
9. Pub L No 111-5, §13405(c), 123 Stat 265.
10. Pub L No 111-5, §13405(d), 123 Stat 266.
11. Pub L No 111-5, §13405(e), 123 Stat 268.
12. 42 USC 13405(a).
13. Pub L No 111-5, §13405(d), 123 Stat 266.
14. Pub L No 111-5, §13405(b), 123 Stat 264.
15. 42 USC 17938.

*Michael S. Khoury of Jaffe Raitt Heuer & Weiss, PC, Ann Arbor and Southfield, practices in the areas of information technology, electronic commerce, intellectual property, and commercial and corporate law.*

*Amy K. Fehn of Wachler & Associates, P.C. has represented physicians and health care organizations in healthcare regulatory and corporate matters for the past eleven years. Prior to graduating from law school, she served as a registered nurse in the coronary care unit and later worked as a clinical systems analyst for the hospital's information systems.*