DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFERS PROPOSED FINAL RULE REGARDING ACCOUNTING FOR DISCLOSURES OF PERSONAL HEALTH INFORMATION, AS REPORTS OF MAJOR DATA BREACHES MOUNT

By: Robert McGuire, Esq.
Podvey, Meanor, Catenacci, Hildner, Cocoziello & Chattman

On February 9, 2011, the United States Department of Health and Human Services (HHS) provided to the Office of Management and Budget a proposed final rule concerning the accounting of disclosures of electronic health records (EHRs) pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act was enacted in 2009 to enhance the protection of personal health information under the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 201 *et seq*. The proposed final rule concerns the portion of the HITECH Act that permits a patient to request that certain health care providers, health plans and health care clearinghouses disclose all instances in which those entities have disclosed that patient's personal health information through EHRs.

Recent Events Regarding the Unauthorized Disclosure of Personal Information -- and Personal Health Information, in Particular

This final rule proposal arrives at a time of rising public concern about unintended disclosure or loss of personal information. Within the past year, numerous high-profile security breaches have made headlines. In June 2010, AT&T reported that hackers had gained unauthorized access to 114,000 e-mail addresses of iPad users who used the carrier's 3G network, which led to the arrest in January 2011 of two persons allegedly responsible for that breach. In October 2010, the social networking website Facebook acknowledged that certain apps that users joined could have transmitted user ID information, even for users who had selected privacy settings that they expected to keep all of their personal information completely private.

Undoubtedly, people might be even more concerned about the unauthorized disclosure of sensitive information regarding their health. And they might be alarmed to learn of recent events that suggest that breaches involving personal health information are not only possible, but perhaps commonplace. In February 2011, RedSpin, Inc., a California security audit firm, released a report entitled "Breach Report 2010: Protected Health Information" that analyzed the 225 data breaches that had been reported to HHS under the HITECH Act. According to RedSpin, those breaches had affected more than

six million people in the United States since August 2009 and had involved citizens in all but seven of the United States. The average breach affected 27,000 persons, and incidents involving portable media (like laptop computers) affected an average of 66,000 people. More than three-quarters of the breaches occurred as part of ten major incidents, and in four of those ten incidents, the unauthorized disclosure was caused by a business associate that had access to the personal health information, rather than the organization that maintained those records. As for the timeliness in disclosing these breaches, the RedSpin report noted that the average delay between a breach and the reporting of that breach to HHS was 82 days (the HITECH Act required such disclosure within 60 days).

Also in February 2011, New York City's Health and Hospitals Corp. confirmed the theft of the confidential personal health data or other sensitive information of approximately 1.7 million New York City patients, hospital staffers, vendors and contractors. The incident in question occurred on December 23, 2010, when thieves stole magnetic data tapes containing that information (perhaps dating back as long as 20 years ago) from an unlocked vehicle owned by the city's medical-records vendor.

The manner in which these breaches occurred is troubling because many major incidents did not result from sophisticated "hacking" of electronic records, but instead occurred because of the theft of common and easily portable storage media like magnetic tapes, laptops and servers.

Recent Enforcement Efforts Pursuant to the HITECH Act

Concern about such disclosures or loss of personal health information has led the government to increase the effort to identify and penalize persons or entities that are responsible for unauthorized disclosures or loss of information. These measures seek to ensure that entities in possession of personal health information and their business associates have effective data-protection procedures in place and abide by them. Within the past year, several large settlements have been reached with parties alleged to have breached their privacy and security obligations with respect to personal health information.

For instance, in July 2010, Rite Aid and its affiliates entered into a $1 million settlement with HHS for potential HIPAA violations after an investigation revealed that pharmacies in the chain might have disposed of prescriptions and pill bottles containing individuals' identifiable personal information in publicly-accessible trash containers. The settlement further required Rite Aid to revise its procedures, train its employees, internally monitor compliance with applicable regulations and to engage an independent third-party assessor to perform compliance reviews to be reported to HHS.

The HITECH Act also authorized state attorney generals for the first time to bring actions for violations of HIPAA obligations. In 2010, Connecticut Attorney General Richard Blumenthal was the first state attorney general to enter into a settlement agreement in connection with HIPAA violations, reaching a settlement for $250,000 with Health Net in connection with a lawsuit that alleged that Health Net had failed properly

to secure private patient medical records and financial information regarding nearly a half-million Connecticut enrollees, and had failed promptly to notify consumers endangered by the breach. Pursuant to the settlement, Health Net also offered two years of credit monitoring for affected participants, obtained $1 million of identity theft insurance, and agreed to reimburse affected individuals for certain other costs. The settlement further provides that Health Net may, under certain circumstances, be required to pay up to an additional $500,000 if the lost information is actually accessed and misused. Aside from monetary payments, Health Net also agreed to implement a corrective action plan, particularly with respect to the protection and encryption of portable media, and to improve employee training.

In January 2011, Vermont Attorney General William Sorrell announced that his office had entered into a $55,000 settlement of another suit, also against Health Net, on behalf of 525 Vermont residents whose personal health information had not been properly protected. That settlement currently awaits court approval.

What Is The HITECH Act, And Who May Be Liable Under It?

The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 and made several changes involving the privacy and security obligations owed to patients under HIPAA, usually referred to as the "HIPAA Privacy Rule" and the "HIPAA Security Rule." In brief, the HIPAA Privacy Rule provides a patient with certain rights over the patient's health information and sets rules and limits on who can look at and receive that health information. The HIPAA Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The HIPAA Security Rule imposes on certain "covered entities" (mainly health care providers, health plans and health care clearinghouses) requirements to ensure the security of protected health information that is kept in electronic format.

The HITECH Act's major provisions include specific reporting requirements that attach in the event of a security breach. Prior to the HITECH Act, no reporting requirements existed in the event of a breach.

The current notification obligations are based on an interim rule that went into effect in September 2009. HHS had submitted and then withdrawn a proposed final breach notification rule to the Office and Management and Budget in the summer of 2010. Until a final breach notification rule is enacted, the requirements of the September 2009 interim rule remain in effect.

Under that interim breach notification rule, notice must be provided in writing to the individuals affected and potentially to certain specified government agencies or the media if the breach involves more than 500 persons in one state. Individual notifications must be provided "without unreasonable delay" and in no case later than sixty 60 days following the discovery of a breach. The notice must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential

harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.

These new notification obligations now include not only "covered entities" under HIPAA, but also business associates and vendors of personal health records. Prior to the HITECH Act, business associates of covered entities had no direct responsibility under HIPAA to protect personal health information. HIPAA, however, had imposed an obligation on covered entities to enter into contracts with business associates that required the business associates to take proper measures to protect this data. Thus, prior to the enactment of the HITECH Act, a business associates could be liable to the covered entity for such breaches under the applicable contract with the covered entities. If a covered entity had failed to require the business associate to enter such a contract, the covered entity was in violation of HIPAA. Now, HHS may proceed directly against a business associate for violations of HIPAA or the HITECH Act.

Aside from making business associates subject to the same breach notification requirements as covered entities, the HITECH Act also requires business associates to provide the same safeguards for electronic health information that covered entities are obliged to employ, and subjects them to the potential penalties. These changes obviously should be of concern to business associates – who typically will have less experience with respect to issues related to the security of personal health information but now must comply with the same obligations that apply to entities that have routinely dealt with HIPPA's Privacy and Security Rules.

Although the HITECH Act's language suggested that the new obligations imposed on business associates would become effective one year after the Act's passage (the Act was passed on February 17, 2009), HHS indicated in a July 14, 2010 Notice of Proposed Rulemaking that the new obligations on business associates would not be enforced by HHS until a final rule was adopted and a subsequent seven-month compliance period had elapsed. See http://edocket.access.gpo.gov/2010/pdf/2010-16718.pdf. (As a note of caution, this Notice does not preclude actions by state attorney generals for violations of HIPAA or the HITECH Act prior to that time.)

As for enhanced enforcement provisions, prior to the passage of the HITECH Act, there were no civil penalties for violations of HIPAA, but the HITECH Act provides for penalties ranging from $100 to $50,000 per offense, and permits penalties for additional violations within a year of the initial offense ranging from $25,000 to $1.5 million. The amount of the fine is based on consideration of a number of factors, including the duration of the breach, the amount of control the party had over the information, and the harm resulting from the breach. As noted previously, the HITECH Act authorizes civil enforcement of HIPAA and the HITECH Act by state attorney generals. Moreover, beginning in February 2012, HHS will be empowered to draft regulations that permit a portion of the civil fines for violations to be distributed to the persons whose data was improperly used or disclosed. Criminal charges may also be brought for violations of these statutes.

The HITECH Act also imposes severe restrictions on the receipt of direct or indirect remuneration by a party in possession of personal health information in exchange for the release of that information, unless the patient has provided prior valid written authorization. In a similar manner, patients must be given a clear opportunity to "opt out" of the potential receipt of fundraising communications from the possessors of personal health information.

The HITECH Act also provides a patient with greater access and control of their health records. If a covered entity maintains a health record in electronic format, a patient has the right under the HITECH Act to secure a copy of that record in electronic format, and the patient may direct the covered entity to transmit that electronic copy to anyone that the patient designates. Conversely, under the HITECH Act, a patient may direct a health care provider in possession of personal health information not to disclose that information to a health plan with respect to any service for which the patient has paid the health care provider in full. The proposed final rule forwarded by HHS on February 9, 2011, with respect to accounting of disclosures of personal health information is an example of HITECH Act's grant to patients of additional control over personal health information.

With HHS's recent forwarding to Office of Management and Budget of the proposed rule as to accounting for disclosures of personal health information and with HHS considering the requirements of a final breach notification rule, the time is fast drawing near when business associates of covered entities will face potential enforcement by HHS of the enhanced penalty provisions set forth in the HITECH Act.

What Can Covered Entities and Business Associates Do to Avoid Liability?

Obviously, the first step any covered entity or business associate should take is to familiarize itself with the requirements imposed by HIPAA and the HITECH Act. An evaluation should be performed as to whether present business practices fail to reflect proper security measures required by the applicable law and involve potential disclosure of protected information in a manner proscribed by HIPAA or the HITECH Act. This review should involve both high-tech solutions (data encryption) and consideration of common sense low-tech measures regarding data security (such as policies prohibiting the removal of storage media that might, for instance, later be left unattended in an unlocked vehicle).

For businesses that deal with this type of information, consideration might be given to the retention of an outside data security specialist to review company policies and procedures. Alternatively, an employer should take steps to ensure that in-house information technology personnel are aware of the legal requirements regarding the privacy and security of personal health information, so that an internal evaluation might be completed and appropriate changes can be made to company practices that do not satisfy the requirements of HIPAA or the HITECH Act. Employers should ensure that employees who use or have access to personal health information are aware of

obligations imposed under HIPAA and the HITECH act, and should provide proper training to existing and new employees to ensure that this information is protected as required by law.

In the event of the discovery of a breach, it is imperative that swift remedial action be taken and that prompt notification be provided to the proper persons and government agencies, as required by law, to minimize any penalties in connection with a data breach.

With respect to financial protection in the event of a breach of obligations under HIPAA or the HITECH Act, some insurers have begun to offer policies that provide coverage in the event of a claim for loss or improper disclosure of protected health information. Any business or person who deals with this kind of information should evaluate the extent to which insurance might be available to protect against or mitigate any damages owed as a result of the loss or disclosure of personal health information.

Finally, because the exposures faced under HIPAA and the HITECH Act are so expansive, businesses that handle any quantity of personal health information should consider consulting counsel familiar with these issues to ensure that these businesses understand the obligations the law imposes on them and the potential consequences for non-compliance in light of the HITECH Act.

Rob McGuire *is a member of the law firm of Podvey, Meanor, Catenacci, Hildner, Cocoziello & Chattman, P.C. located in Newark, New Jersey. Podvey Meanor's practice emphasizes general commercial litigation, business law, land use, the prosecution and defense of consumer fraud actions, professional liability and products liability defense. The firm also performs corporate investigations and defends allegations of white collar crime and other criminal charges. Rob can be reached at (973) 623-1000 or at rmcguire@podvey.com.*