

HITECH Raises the Stakes on HIPAA Compliance

Author: Robert Belfort

Since the Health Insurance Portability and Accountability Act (“HIPAA”) went into effect several years ago, privacy advocates have dismissed the law as a “paper tiger.” Among the criticisms of HIPAA were that the privacy and security rules do not apply to many organizations that routinely handle large amounts of health information, the potential sanctions (except in the rare cases of criminal conduct) are not sufficiently severe and the United States Department of Health and Human Services (HHS) Office of Civil Rights has never imposed a single civil penalty.

Each of those criticisms have been addressed by Congress with the enactment of the Health Information Technology for Economic and Clinical Health Act (“HITECH”), which was part of the \$787 billion federal stimulus bill signed by President Obama on February 17, 2009. HITECH strengthens and expands HIPAA’s privacy and security requirements in five key areas described below.

As a result of HITECH, health plans, health care providers and other covered entities will have to review and potentially modify their privacy and security policies, employee training programs, business associate agreements, breach notification protocols and internal auditing plans. They may also have to modify existing data sharing arrangements that are no longer permissible. Business associates and personal health records (PHR) vendors will have to prepare for the heightened scrutiny that comes with direct regulation by HHS and the Federal Trade Commission (FTC), respectively. Other organizations will have to carefully monitor the future extension of HIPAA to a wider range industry participants, which is signaled by HITECH.

Direct Application of HIPAA to Business Associates

When issuing the HIPAA privacy and security rules, HHS concluded it was without statutory authority to directly regulate the many vendors that receive, use, maintain and disclose protected health information on behalf of health care providers and health plans. In an effort to bring these vendors within HIPAA’s orbit, HHS deemed them “business associates” and required covered entities to impose contractual limitations on their use and disclosure of protected health information. But business associates were not directly subject to HHS oversight or penalties.

HITECH directly regulates business associates for the first time. While not subjecting business associates to all of the obligations of covered entities (such as providing privacy notices), the statute requires business associates to comply with the HIPAA security rule provisions mandating administrative, physical and technical safeguards. It also requires them to adhere to the terms of their business associate agreements, including the restrictions on the use and disclosure of protected health information. Business associates are subject to the same civil and criminal penalties as covered entities for violating these requirements. This exposes technology vendors, practice management companies, transcription

services, billing services, attorneys, accountants and many other types of business associates to direct regulation under HIPAA. The change becomes effective one year after HITECH's enactment. HHS and the FTC are directed to study the potential expansion of HIPAA to organizations that are neither covered entities nor business associates.

Security Breach Notification Mandate

HIPAA requires covered entities to mitigate the potentially harmful effects of improper disclosures. But it does not expressly mandate notification of affected individuals in the event of any security breach. HITECH establishes the first national data security breach notification law. It requires covered entities to notify affected individuals of a breach involving "unsecured" protected health information. Business associates are required to notify covered entities of such breaches. Unlike many comparable state laws, HITECH covers information maintained in any form, not only electronic data. HHS is directed within 60 days of HITECH's enactment to identify technologies that, if utilized, will ensure that information is deemed secure.

Covered entities must notify affected individuals without "unreasonable delay" and in no event more than 60 days after discovery of the breach. Notification must be made by letter or by e-mail if the individual has expressed a preference to receive notices electronically. Alternative forms of notice (such as a website posting) are permissible when the covered entity lacks adequate contact information. If more than 500 individuals in a state are affected, notice must be provided to "prominent media outlets." Notice must also be provided to HHS. If more than 500 individuals are affected, HHS will list the breach on its website. HITECH specifies the content of the notice.

A comparable notification obligation is imposed on "vendors of personal health records," which are defined as entities that maintain electronic records comprised of health information drawn from multiple sources that are controlled by the individual. PHR vendors are generally not regulated by HIPAA. In addition to notifying affected individuals of a breach, PHR vendors must also inform the FTC. A breach is defined as the acquisition of unsecured identifiable health information by any person without the individual's authorization. The requirements regarding the content and timing of the notice are the same as those imposed on covered entities.

HHS and the FTC are directed to issue interim final regulations implementing the security breach notification requirements within 180 days of HITECH's enactment. The requirements will become effective 30 days after the publication of such regulations.

The HITECH provisions overlap with, but differ from, the many state notification laws that have been enacted over the past ten years. Covered entities and PHR vendors will have to carefully analyze the combined effect of HITECH and these state laws in developing security breach action plans.

New Restrictions on the Use and Disclosure of Protected Health Information

HITECH restricts currently permissible uses and disclosures of protected health information in a few important ways:

- A covered entity is prohibited from receiving remuneration for the disclosure of protected health information without the individual's authorization, except for disclosures for limited purposes such as public health, treatment or research. Payment for research disclosures may not exceed the cost of preparing and transmitting the data. Currently, HIPAA does not restrict

payment arrangements for data if the disclosure fits within a HIPAA exception. HHS is directed to issue regulations implementing and potentially tightening the new restrictions. The limitation becomes effective six months after the date these regulations are promulgated.

- HIPAA currently carves out of the definition of prohibited “marketing” certain promotional communications to individuals. For example, a covered entity may use protected health information to inform an individual about the entity’s own health care products or services. These communications are no longer permissible without the individual’s authorization if the covered entity making the communication receives payment from another party for doing so. For instance, a pharmacy may no longer send a letter to customers about a new drug if the pharmacy receives compensation from the drug’s manufacturer for sending the letter. An exception applies if the communication involves a drug the individual is already taking and certain conditions are satisfied. This restriction becomes effective six months after HHS issues implementing regulations.
- Except in limited circumstances such as treatment, HIPAA requires covered entities to use and disclose the “minimum necessary” information. In the past, the determination of the minimum necessary data set was left to the judgment of the covered entity. HITECH requires covered entities to use or disclose only a “limited data set” if sufficient to carry out the intended purpose. A limited data set excludes names, street addresses, social security numbers and other identifiers but is not fully “de-identified” in accordance with HIPAA standards. HHS is also directed to issue regulations within 18 months of HITECH’s enactment providing additional guidance on what constitutes the minimum necessary information. The limited data set requirement sunsets when such regulations are issued.

New Patient Rights

HITECH grants individuals several new rights regarding their protected health information:

- Covered entities must honor an individual’s request not to share information with the individual’s health plan for payment or health care operations if the individual is paying the full cost of the service to which the information relates. Currently, covered entities must process such requests but are not obligated to grant them.
- One year after HITECH’s enactment, covered entities maintaining electronic health records are required to give individuals copies of their records in electronic form.
- Covered entities maintaining electronic health records are obligated, at an individual’s request, to provide an accounting of all disclosures of the individual’s protected health information made for treatment, payment and health care operations during the prior three years. Disclosures for such purposes are exempt from HIPAA’s current accounting requirement. If a covered entity acquired an electronic health record system on or before January 1, 2009, the new accounting requirement becomes effective January 1, 2014. For covered entities purchasing such a system after January 1, 2009, the requirement takes effect on January 1, 2011 or the date of the purchase, whichever is later.
- Fundraising communications must notify individuals that they have a right to opt out of any future fundraising solicitations.

Heightened HIPAA Enforcement

HITECH ratchets up the potential sanctions that may be imposed under HIPAA in several key respects:

- HITECH establishes a tiered system of civil penalties based on the nature of the improper conduct. In situations where the covered entity does not know it violated HIPAA, the current maximum penalty of \$100 per violation, up to \$25,000 per year, for each type of violation will be applicable. If the violation is due to “reasonable cause,” the maximum penalty rises to \$1,000/\$100,000. If the violation is due to “willful neglect,” the maximum penalty is \$500,000/\$1.5 million. The increased penalties are effective immediately. Beginning two years after HITECH’s enactment, HHS is required to impose civil penalties on a covered entity if the violation is due to “willful neglect.”
- The GAO is directed to prepare a report within 18 months of HITECH’s enactment recommending a methodology for allowing affected individuals to share in civil monetary penalties imposed under HIPAA. HHS must adopt such a methodology within three years of HITECH’s enactment. Once implemented, this provision will increase the incentive for individuals to file privacy and security complaints with HHS, mirroring the impact of the False Claims Act’s *qui tam* authority.
- Effective immediately, State Attorneys General are granted authority to bring civil actions to enforce HIPAA. HHS is directed to evaluate how to enable affected individuals to share in penalties collected for violating HIPAA.
- HITECH “clarifies” that criminal penalties may be imposed under HIPAA on any individual or entity that wrongly obtains or discloses protected health information maintained by a covered entity. This provision is intended to end the debate over whether HIPAA authorizes the imposition of criminal penalties only on covered entities.
- HHS is directed to conduct periodic audits of covered entities and business associates to evaluate HIPAA compliance. In the past, HHS enforcement consisted largely of responding to complaints.