

Stimulus package affects health data privacy and security

Provisions increase compliance duties of covered entities, as well as exposure to new liability risks.

by **Nancy L. Perkins, JD**

New requirements for protection of personal health information included in the recently enacted economic stimulus legislation will significantly affect members of the health care industry — as well as entities with which they work.

These provisions increase the compliance stakes for covered entities regulated



Nancy L. Perkins, JD

by the Department of Health and Human Services privacy and security rules implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, they expose business associates of such covered entities, as well as vendors of certain personal health information, to new liability risks.

The pertinent provisions of the stimulus legislation are part of the initiative for health information technology that is designed to streamline the sharing of health information through the use of electronic medical records. To ensure the privacy and security of individually identifiable health information (protected health

information, or PHI) in this context, Congress expanded on many of the obligations and enforcement mechanisms under the HIPAA privacy and security rules.

This article provides a high-level summary of some of the more pertinent provisions.

Breach notifications

Following the lead of many states that have enacted laws requiring notification to law enforcement and affected individuals of breaches of personal information security, Congress included in the stimulus legislation similar breach notification requirements with respect to health information.

Under these requirements, HIPAA-covered entities (health care providers engaging in certain electronic transactions, health plans and health care clearinghouses), their business associates and vendors of personal health records must notify affected individuals of a breach of unsecured PHI or personal health record information. In addition, covered entities and their business associates must provide breach notifications to HHS (vendors must notify the Federal Trade

Commission) and, if more than 500 individuals are affected in a particular area, also notify prominent media outlets serving that area.

HHS will post on its Web site a list of each covered entity involved in a breach affecting more than 500 individuals.

Marketing

Currently, the HIPAA privacy rule generally prohibits the use or disclosure of PHI for marketing purposes without an individual's written authorization. Marketing generally means providing a communication that encourages the recipient to purchase or use a particular product or service.

However, such a communication is not marketing if it is made for purposes of: (1) describing a health-related product or service that is provided by, or included in a plan of benefits of, the covered entity; (2) providing treatment to the recipient; or (3) case management or care coordination, or directing or recommending alternative treatments, therapies, health care providers, or settings of care — even if the covered entity is paid by a third party to make the communication.

CO-EDITORS



Alan E. Reider

Allison Weber Shuren

Under the new stimulus legislation, a covered entity is prohibited to make any of the three above-referenced “excepted” types of communications in exchange for payment (direct or indirect) without an individual authorization, unless: (1) the communication “describes only a drug or biologic that is currently being prescribed for the recipient of the communication” and (2) the payment received by the covered entity in exchange for making the communication is “reasonable in amount.” HHS is charged with defining, by regulation, what constitutes a reasonable amount in this context.

Notably, the stimulus legislation states that “direct or indirect payment shall not include any payment for treatment (as defined in [the HIPAA privacy rule]) of an individual.” However, HHS has expressly opined that: “It is not marketing for a doctor to make a prescription refill reminder, even if a third party pays for the communication. The prescription refill reminder is considered treatment. The communication is therefore excluded from the definition of marketing and does not require a prior authorization.”

Apparently, the stimulus legislation overrides this HHS interpretation of refill reminders as treatment, at least with respect to the requirement to obtain an individual authorization if the refill reminder is made in exchange for payment beyond a reasonable amount.

Sales of PHI

The stimulus legislation prohibits covered entities and their business associates from receiving payment in exchange for PHI without an individual authorization that refers to the payment, unless the purpose of the exchange is for: (1) research, and the price charged reflects the costs of preparation and transmittal of the data; (2) treatment; (3) due diligence in connection

with the sale, transfer or merger of the covered entity; (4) permissible contracted work pursuant to a business associate agreement; (5) the provision of a copy of the PHI to the individual to whom it pertains; or (6) other purposes as determined by HHS.

Business associate liability

Currently, business associates of covered entities are not subject to direct liability under HIPAA or its implementing rules; rather, they are liable for breach of their required business associate contracts with HIPAA-covered entities.

The stimulus legislation changes that legal framework. It applies the pertinent provisions of both the HIPAA privacy rule and the security rule — including the enhancements to those provisions in the stimulus legislation — directly to business associates, such that the civil and criminal penalties for violating those provisions may be imposed on business associates in the same manner as they apply to covered entities. This could well alter the dynamics of negotiating business associate agreements, particularly in light of the new enforcement provisions included in the stimulus bill, as described below.

Enhanced enforcement

Currently, only the HHS has authority to enforce the HIPAA regulations, except with respect to criminal conduct, which is subject to Department of Justice investigation and the imposition of criminal penalties.


The stimulus legislation grants new authority to both HHS and the Department of Justice with respect to penalties (and increases the amount of potential civil penalties imposed). The legislation also provides that any civil monetary penalties or monetary settlements obtained are to be transferred to the HHS Office for Civil Rights for use in its future privacy and security enforcement efforts.

In addition, the stimulus legislation authorizes state attorneys general to bring civil actions on behalf of state residents who allegedly have been harmed by HIPAA violations — unless HHS has already initiated action regarding the same alleged violation, for as long as the HHS action is pending. State attorneys general may pursue injunctive relief, statutory damages and attorneys’ fees. The damages obtained in a state attorney general action could be as much as \$100 per violation, with a maximum of \$25,000 for all violations of an identical requirement or prohibition during a single calendar year.

Studies and regulations

The stimulus legislation requires that several studies be undertaken and that HHS and the Federal Trade Commission promulgate a variety of regulations to implement the provisions relevant to their respective jurisdictional authority.

In general, the health information privacy and security provisions of the legislation take effect within 1 year of enactment, ie, on Feb. 17, 2010, and much of the regulatory work is required to be done before that date. Covered entities, their business associates, medical researchers and others with an interest in individually identifiable health information would be well advised to seek counsel on the potential impact of the new legislation on their activities and plans, as well as advice on how they might influence the content of the forthcoming implementing regulations.

The significance of the legislation and those regulations may be far greater for certain entities than is suggested by this short summary of selected provisions. 

Nancy L. Perkins, JD, can be reached at Arnold & Porter LLP, 555 12th St. NW, Washington, DC 20004-1206; 202-942-5065; e-mail: nancy.perkins@aporter.com.