JONES DAY

FEBRUARY 2009

STIMULUS BILL SUBSTANTIALLY REVISES HIPAA'S PRIVACY AND SECURITY RULES

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (the "Act"). Among many other things, the Act dedicates substantial resources to health information technology and investment in infrastructure to allow for and promote the electronic exchange and use of health information. Title XIII of Division A and Title IV of Division B of the Act are commonly referred to as the "Health Information Technology for Economic and Clinical Health Act" or "HITECH Act." This *Commentary* provides an overview of the key amendments to the privacy and security regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") that are contained in Subtitle D of the HITECH Act. Subtitle D also sets forth a few new defined terms, which are highlighted in text boxes below. Although most of the Act's provisions will take effect one year after enactment of the law (February 17, 2010), a few provisions have different timelines, which are also highlighted below.

DIRECT DUTIES FOR BUSINESS ASSOCIATES

Critics of HIPAA have long complained that HIPAA's failure to impose direct obligations on business associates who routinely handle protected health information created a jurisdictional impediment to privacy and security enforcement. That impediment has now been removed. The Act provides that HIPAA security provisions as well as certain additional privacy and security provisions set forth in the Act will apply to business associates in the same manner that they apply to covered entities, and that such requirements must be incorporated into existing and future business associate agreements between business associates and covered entities. Currently, covered entities (through business associate agreements) are responsible for contractually obligating their business associates to comply with requirements relating to use and disclosure of protected health information. The Act now

subjects business associates to the administrative, physical, and technical safeguard requirements set forth in the HIPAA security rule, as well as its requirement to maintain written policies and procedures. Similarly, the Act provides that the civil and criminal penalties that may arise if a covered entity violates the privacy and security provisions would also apply to business associates who violate the security standards or the terms of their business associate agreement.

BREACH NOTIFICATION

Covered Entities and Business Associates. HIPAA has never contained a requirement that a covered entity must notify individuals in the event of a data security breach involving their protected health information. Thus, covered entities faced with such a breach needed to determine whether notification was warranted by HIPAA's requirement to mitigate harm to individuals or was otherwise required by state security breach notification laws. Under the Act, notification will no longer be a matter of discretion.

The Act requires covered entities to notify each individual whose *unsecured protected health information* has been accessed, acquired, or disclosed as a result of a *breach*. If a business associate discovers the *breach*, it must notify the covered entity within 60 days and identify the individual(s) whose information has been compromised. The *breach* will be treated as discovered (whether by a covered entity or business associate) as of the first day the *breach* is known or should reasonably have been known by any employee or agent of the covered entity or business associate (as the case may be). Notices must be given in a timely fashion, and in no case later than 60 calendar days after discovery (with a limited exception for delays relating to law enforcement purposes). The covered entity or the business associate (as the case may be) has the burden of demonstrating that its required notifications have been given.

breach – the unauthorized acquisition, access, use, or disclosure of protected health information that compromises the security or privacy of such information, except where the person to whom the information is disclosed would not reasonably have been able to retain such information or in certain specified circumstances of inadvertent disclosure or unintentional acquisition of the information.

unsecured protected health information – protected health information that is not secured through the use of technology or methodology specified by the Secretary.

The Act describes with some specificity how notice should be given to individuals, depending on whether a last known address or other contact information is available. Media notice is also required if the *breach* involves information pertaining to more than 500 individuals, along with immediate notice to the Secretary of Health and Human Services (the "Secretary"), which will then be posted by the Secretary on the Department of Health & Human Services ("DHHS") web site. If fewer than 500 individuals are involved, the covered entity is not required to provide the Secretary with immediate notice, but instead may maintain a log that is submitted annually to the Secretary. The Act provides some details on the content of the notice, including a description of the *breach* and the types of *unsecured protected health information* that were involved, the steps individuals should take to protect themselves from potential harm, a description of what steps the covered entity is taking, and the contact information for questions.

The Act directs the Secretary to consult with stakeholders and issue guidance within 60 days specifying the technologies and methodologies that render protected health information secured or, in the words of the Act, "unusable, unreadable or indecipherable" to unauthorized individuals. Further, to carry out the *breach* notification provisions, the Act directs the Secretary to promulgate interim final regulations within 180 days. The provisions will apply to *breaches* that are discovered on or after 30 days of publication of the regulations.

The *breach* notification provisions in the Act do not preempt state security *breach* notification laws that are more restrictive. Clearly, not all *breaches* of *unsecured protected health information* will trigger notification obligations under state laws since most states require the *breach* to involve identifying information such as Social Security number, credit card number, bank account number, or the like. But, when state notification laws are triggered, a health care entity will now have both federal and state notice requirements with which to comply. This will be a challenge in some instances because the notification obligations may be inconsistent.

Vendors of PHR and Related Entities. Vendors of *personal health records* ("PHR") and entities that offer products or services through the web site of a PHR vendor or a covered entity that offers PHRs, and entities that access information in or send information to a PHR all face notice requirements similar to those described above for covered entities and business associates in the event of a *breach of security*. Notice must be given to the individual whose information has been compromised (if a citizen or resident of the United States) and to the Federal Trade Commission ("FTC"). The FTC will in turn notify the Secretary. Failure to comply with the notice requirements will be treated as an unfair and deceptive act or practice in violation of the Federal Trade Commission Act. Further, the Act mandates that the FTC promulgate interim final regulations within 180 days to carry out these requirements. The provisions will apply to *breaches of security* that are discovered on or after 30 days of publication of the regulations.

breach of security – acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual.

personal health record – an electronic record of individually identifiable health information that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

PHR identifiable health information – individually identifiable health information as defined under HIPAA that is contained in a personal health record and includes information that is provided by or on behalf of the individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

unsecured PHR identifiable health information – PHR identifiable health information that is not protected through the use of technology or methodology specified by the Secretary.

ACCOUNTING OF DISCLOSURES

Under the existing HIPAA regulations, a covered entity must account for its (and its business associates') disclosures of protected health information. Many disclosures, however, have been excepted from this disclosure requirement, including disclosures that are made for treatment, payment, or health care operations purposes. The Act significantly expands the disclosures required to be reported in an accounting of disclosures. Under the Act, covered entities that use or maintain *electronic health records* will need to account for disclosures made for treatment, payment, and health care operations purposes. Individuals will have the right to receive the accounting for this type of disclosure for three years (as opposed to six years for other disclosures). This change picks up all disclosures made in the clinical setting as well as all disclosures to business associates (which were formerly excepted as health care operations disclosures). The Secretary has been directed to promulgate standards within six months to assist in implementation of this requirement. Recognizing that this drastic change requires technological solutions, the compliance date for covered entities that "acquired" an *electronic health record* as of January 1, 2009, is January 1, 2014. For covered entities that acquire *electronic health records* after January 1, 2009, the compliance date is the later of January 1, 2011, or the date upon which the *electronic health record* is acquired.

electronic health record – an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Further, the Act allows covered entities to account for disclosures (i) by providing the accounting for all disclosures by the covered entity and its business associates or (ii) by providing the accounting for all disclosures by the covered entity and providing a list of all of the covered entity's business associates, including contact information for the business associates. A business associate included on such a list must provide an accounting of disclosures made by the business associate upon request made by an individual directly to the business associate.

MINIMUM NECESSARY

The Act refines the rules regarding limitation of disclosures to the "minimum necessary" and calls for the Secretary to provide guidance. The Secretary has been instructed

to take into consideration the "information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease" in publishing such guidance. In the interim, covered entities will be treated as being in compliance if the information disclosed consists of the limited data set or the "minimum necessary" to accomplish the purpose of the use or disclosure. Also, the Act indicates that the disclosing entity "shall determine what constitutes the minimum necessary" to accomplish the purpose of the disclosure. It is unclear whether this statement was intended to remove the covered entity's ability to rely on the requesting party to determine the minimum necessary in certain situations (*e.g.*, requests by public officials or other covered entities) as set forth in 45 CFR 164.514(d)(3)(iii).

BUSINESS ASSOCIATE AGREEMENT REQUIRED FOR OTHER ENTITIES

The Act requires organizations that provide data transmission of protected health information and require regular access to such protected health information (*e.g.*, health information exchanges and regional health information organizations) to enter into a business associate agreement with the covered entities that provide protected health information.

MARKETING

With certain exceptions, HIPAA requires patient authorization for use of protected health information for marketing purposes. Certain marketing-type activities, however, were excepted from HIPAA's definition of "marketing" because they were deemed to be part of treatment or health care operations. The Act narrows the ability to use protected health information in connection with these formerly permissible quasi-marketing activities if the covered entity receives direct or indirect payment from a third party in connection with the communication. The Act sets forth a limited exception to the general prohibition that includes, among other things, that the payment is "reasonable in amount," a term that is to be defined by the Secretary by regulation.

ENHANCEMENT OF INDIVIDUALS' RIGHTS

The Act requires covered entities and business associates to provide individuals whose protected health information is stored in an *electronic health record* with electronic copies of the information for no more than the labor cost incurred in responding to the request for the copy. The Act requires that covered entities comply with requests from individuals to restrict disclosures of their protected health information if (i) the restriction relates to disclosure to a health plan for payment or health care operations (as opposed to treatment) purposes, and (ii) the protected health information pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full, unless the disclosure is otherwise required by law. The Act also provides that written fundraising communications must provide the recipient with the option to elect not to receive any further communications in a "clear and conspicuous" manner.

ENFORCEMENT

Another significant amendment set forth in the Act relates to HIPAA enforcement. The Act takes HIPAA enforcement from a reactive, complaint-driven system to a more proactive system, driven by audits and enforcement activities that are funded by civil monetary penalties. The Act requires the Secretary to provide for periodic audits to ensure that covered entities and business associates are in compliance with the requirements of the Act. The Secretary is also directed to establish a methodology under which an individual who is harmed by an offense may receive a portion of any civil monetary penalty or monetary settlement collected with respect to such offense. The Act also provides for a tiered increase in the amount of civil monetary penalties and allows for enforcement through state attorneys general (with the Secretary retaining the right to intervene). It is noteworthy that these provisions take effect immediately.

PROHIBITION ON SALE OF PROTECTED HEALTH INFORMATION

The Act prohibits a covered entity or business associate from receiving remuneration in exchange for any protected health information except where the individual in question has authorized it or where certain specified purposes are served. The Act directs the Secretary to issue regulations to carry out this provision within 18 months and provides for it to take effect six months after issuance of the regulations.

PRIVACY EDUCATION

The Act directs the Secretary to designate an individual for each regional office of DHHS to provide guidance and education to covered entities, business associates, and individuals on their rights and responsibilities relating to the security and privacy requirements. Furthermore, the Office of Civil Rights within the DHHS is directed to develop a national education initiative to, in the words of the Act, "enhance public transparency regarding the uses of protected health information."

CONCLUSION/WHAT YOU SHOULD DO

The Act provides for substantial amendments to the privacy and security regulations under HIPAA and imposes direct obligations on business associates. It also calls upon the Secretary to issue a great deal of guidance, regulations, and reports in the coming months in furtherance of the Act's mandates. Both covered entities and business associates should closely follow these activities to determine what obligations will apply to them. For example, covered entities will likely need to revise their policies concerning disclosures to comply with the expected guidance on the revised "minimum necessary" standard and will need to change their accounting of disclosure-reporting procedures when that guidance is published. The Notice of Privacy Practices will also need to be updated to reflect these changes. If they haven't already done so, covered entities should adopt policies and procedures for responding to security breaches.

Covered entities and business associates will need to revise their business associate agreements to comply with the Act. Business associates should also adopt written policies and procedures to comply with the HIPAA security obligations that are now imposed on them. Finally, in order to prevent security breaches and minimize the harm that can result from them, all entities that handle protected health information should explore available methods and technologies to render this information unusable, unreadable, or indecipherable to unauthorized individuals and should deploy such methods and technologies throughout their operations as soon as practical.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Jeffrey L. Kapp
1.216.586.7230
jlkapp@jonesday.com

Kevin D. Lyles
1.614.281.3821
kdlyles@jonesday.com

Asha B. Scielzo
1.202.879.5449
abscielzo@jonesday.com