HEALTH CARE
Legal News Alert℠
FOLEY
FOLEY & LARDNER LLP
FEBRUARY 2009

Stimulus Package Dramatically Alters HIPAA Privacy and Security

On February 17, 2009, President Barack H. Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA), commonly referred to as the federal stimulus package. As summarized in our Legal News Alert issued on February 18, 2009 (http://www.foley.com/publications/pub_detail.aspx?pubid=5726), a significant portion of the ARRA's stimulus expenditures and measures are related to health information technology (HIT) and incentives to adopt electronic health record (EHR) systems. Adoption of EHR systems is believed to be critical to improvement in quality of care and ultimate cost savings to the health care system. However, the government recognizes that widespread adoption of HIT and EHR systems will not occur unless there is public assurance that the privacy and security of patient information in such systems is protected. In recognition of this, the ARRA significantly expands the scope of the privacy and security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) pursuant to the Health Information Technology for Economic and Clinical Health Act's (HITECH Act) provisions within the ARRA.

The HITECH Act impacts both covered entities and their business associates as well as vendors of personal health records and health information exchange organizations that are not covered under HIPAA. This Legal News Alert only focuses on key provisions in the HITECH Act that impact covered entities and their business associates.

The HITECH Act will require covered entities and their business associates to revise many of their policies and procedures and will likely require them to amend their business associate agreements. However, the provisions with the most significant, far-reaching impact will be the new mandatory breach notification requirements coupled with a new, heightened enforcement scheme. In addition to increased penalties under the HITECH Act, patients will now be able to have their medical privacy breach allegations heard in court through state attorney general enforcement authority. The potential exposure to covered entities for penalties, fines, and damages is significantly increased under the HITECH Act. Moreover, under the HITECH Act, HIPAA privacy and security provisions will apply directly to business associates. Business associates also will be subject to the same heightened civil and criminal penalties that apply to covered entities.

The following summarizes some of the key requirements of the HITECH Act. Most of the HITECH Act's provisions take effect 12 months from the date of enactment. However, certain requirements have different effective dates, which are indicated below.

Security Breach Notification
Currently, HIPAA does not directly obligate covered entities to notify patients of unauthorized uses or disclosures of their protected health information (PHI). Absent an applicable state security breach notification law, covered entities have had the discretion to determine whether their duty to mitigate known harm that could result from an unauthorized use or disclosure would trigger the duty to notify patients. The HITECH Act removes most of this discretion and mandates patient notification in certain circumstances.

The HITECH Act requires that patients be notified of any unauthorized acquisition, access, use, or disclosure of their unsecured protected health information (Unsecured PHI) that compromises the privacy or security of such information, with some exceptions related to unintentional or inadvertent use or disclosure by employees or authorized individuals within the "same facility." The HITECH Act specifies the timeliness of such notifications (i.e., "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach") and details the information that must appear in the notification to affected patients.

The U.S. Department of Health and Human Services (HHS) is required to define the term "Unsecured PHI" within 60 days. If such guidance is not issued, the HITECH Act defines Unsecured PHI as any PHI that is not secured by a technology standard that renders it unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute. If a breach affects 500 patients or more, it must be reported to HHS, which will post the name of the breaching entity on its public Web site. Breaches affecting 500 patients or more who reside in the same area must be reported to the local media.

These new security breach notification requirements apply to covered entities and require business associates to notify covered entities of any unauthorized acquisition, access, use, or disclosure of Unsecured PHI they hold on behalf of the covered entity, including the identity of each individual who is the subject of the Unsecured PHI.

The security breach notification requirements apply not only to unauthorized disclosures of Unsecured PHI to outside third parties, but also to unauthorized internal access to such PHI. This means that unauthorized employee "snooping" into medical records could trigger

the notification requirements.

HHS has 180 days to issue regulations to implement the security breach notification requirements, and these requirements become effective for breaches discovered 30 days after the date HHS issues the regulations.

Heightened Enforcement, Increased Penalties, and Audits
Under the current HIPAA enforcement scheme, the focus has been on resolution of alleged non-compliance in collaboration with the covered entity at issue via corrective action. That focus will now be changed. The HITECH Act contains a section entitled "Improved Enforcement" and imposes mandatory penalties for violations of HIPAA that are due to "willful neglect." This section also requires HHS to investigate formally any complaints that are preliminarily determined to involve potential willful neglect.

The HITECH Act increases civil penalty amounts based upon the level of intent and neglect (i.e., whether the violation was made without knowledge, due to reasonable cause, or due to willful neglect). For violations determined to be made without knowledge, penalties start at $100 per violation and are not to exceed $25,000. For violations based on reasonable cause, penalties start at $1,000 per violation and are not to exceed $100,000. For violations due to willful neglect, penalties start at $10,000 and are not to exceed $250,000. For violations due to willful neglect that are not corrected, penalties start at $50,000 and are not to exceed $1.5 million. The HITECH Act specifically allows the Office for Civil Rights (OCR) to continue to use corrective action without a penalty, but only in situations where the violation was made without knowledge.

In addition to extending civil and criminal liability under HIPAA to business associates, the HITECH Act clarifies that criminal penalties may apply to an individual or employee of a covered entity that obtains PHI without authorization.

The HITECH Act provides that any penalties collected will be used to support the enforcement activities of the OCR. Individuals whose PHI was the subject of an OCR enforcement action will ultimately receive a percentage of any penalties.

The current version of HIPAA does not provide for a private right of action, meaning that patients cannot file suit in court based upon alleged HIPAA violations. The HITECH Act heightens HIPAA enforcement by authorizing state attorneys general to file suit on behalf of their residents. Courts will be able to award damages, costs, and attorneys' fees related to violations of HIPAA.

Lastly, the HITECH Act requires HHS to conduct periodic audits of both covered entities and business associates to ensure HIPAA compliance.

Most of these provisions become effective upon the date of enactment of the HITECH Act, with further guidance to be issued for certain requirements.

Other Provisions Impacting Business Associates
Currently, business associates are not governed by HIPAA, but rather are only contractually restricted in their use and disclosure of PHI pursuant to their business associate agreements. As noted above, this will change because the HITECH Act applies certain HIPAA provisions to business associates. For example, business associates will have to comply with the administrative, physical, and technical safeguards under the HIPAA Security Rule, among other requirements. Business associates will have to report security breaches subject to the notification requirements to covered entities and provide certain information in such reports. Further, business associates will be subject to civil and criminal penalties under HIPAA. The HITECH Act also specifies that business associates can be subject to civil and criminal penalties if they fail to take action upon becoming aware of covered entity activities that do not comply with HIPAA.

The HITECH Act's new provisions regarding accounting of disclosures from an EHR (see below) also impact business associate relationships. Covered entities may choose either to account for business associate disclosures or to provide a list of all business associates to an individual for that individual to directly request an accounting from such business associates.

The provisions that give patients the right to access their PHI in an electronic format also may impact business associates who maintain such information on behalf of covered entities.

The HITECH Act affirmatively requires that new provisions be incorporated into existing business associate agreements. The business associate requirements become effective 12 months after the date of enactment of the HITECH Act.

Accounting Requirements
HIPAA currently requires covered entities to account for disclosures with certain exceptions and to record information about such disclosures in a log. The most significant exception is disclosures made for purposes of treatment, payment, or health care operations. These disclosures were not subject to the accounting requirements because they were categorized as the type of disclosures that patients would expect to occur. Now, in addition to accounting for the disclosures currently required to be logged, the HITECH Act requires covered entities to account for disclosures of PHI used or maintained in an EHR system that are related to treatment, payment, or health care operations for a period of three years prior to the date of the request.

The impact of the new accounting requirements will depend upon the audit trail capabilities of a covered entity's EHR system as well as the information that will have to be collected and provided to patients as part of the accounting. HHS is required to issue regulations on the information that must be collected as part of an accounting audit.

The effective date for current EHR users is January 1, 2014. For those who acquire an EHR system after January 1, 2009, the effective date is January 1, 2011, or the date the EHR system is acquired, whichever is later.

Right to Request Restriction
Although HIPAA provides individuals with the right to request covered entities to restrict uses or disclosures of their PHI for treatment, payment, health care operations, or certain other purposes, HIPAA currently does not require that covered entities agree to such a request. The HITECH Act requires covered entities to comply with requests from individuals that their PHI not be disclosed to a health plan, if the purpose for the disclosure is not related to treatment, and the health care services to which the PHI applies have been paid for out-of-pocket in full. Otherwise, individuals cannot force covered entities to restrict uses or disclosures of their PHI for treatment, payment, or health care operations purposes.

These requirements become effective 12 months after enactment of the HITECH Act.

Limited Data Sets and Minimum Necessary
HIPAA currently requires covered entities to use, disclose, or request the minimum necessary PHI to accomplish the intended purpose, but provides no further defining criteria. The HITECH Act imposes a new requirement to the "minimum necessary" standard. Specifically, covered entities are required "to the extent practicable" to limit uses, disclosures, and requests for PHI to a "limited data set," or if needed, to the minimum necessary to accomplish the intended purpose. A limited data set under HIPAA is a subset of PHI that is stripped of the majority of identifiers and is virtually de-identified. Although the removal of the identifiers required to create a limited data set will likely render the information ineffective to meet the purposes of most uses, disclosures, or requests to access PHI, the HITECH Act requires application of these restrictions "to the extent practicable."

The limited data set requirements go into effect 12 months from the enactment of the HITECH Act and will sunset once HHS issues guidance (due within 18 months of enactment of the HITECH Act) as to what constitutes the minimum necessary.

Prohibition on Sale of PHI or Electronic PHI
HIPAA does not currently directly prohibit sales of PHI or electronic PHI (E-PHI). To address the lack of restrictions, the HITECH Act now prohibits a covered entity or business associate from selling (i.e., receiving any remuneration directly or indirectly) an E-PHI or PHI without a valid authorization unless:

- The sale is for public health activities
- The sale is for research activities and the price charged reflects the cost of preparation and transmittal of the data
- The sale is for the treatment of the individual
- The purpose for the exchange of PHI is related to the sale, transfer, or merger of all or part of a covered entity
- The sale is for a business associate function pursuant to a business associate agreement
- The sale is to provide an individual with a copy of his/her PHI
- The sale is for any other activity deemed necessary and appropriate by the Secretary of HHS

HHS is required to promulgate regulations within 18 months after enactment of the HITECH Act. These provisions become effective six months after the regulations are issued.

Conditions on Marketing Communications
HIPAA currently defines "marketing communications" as a communication about a product or service that encourages recipients of the communication to purchase or use that product or service. Communications for marketing purposes can only be made with a patient's prior written authorization. However, there are three exceptions to the definition of marketing as follows: (i) communications a covered entity makes about its own health care products or services; (ii) communications for treatment purposes; and (iii) communications for purposes of case management or care coordination or to recommend alternative treatments, therapies, health care providers, or settings of care. If a communication that otherwise meets the definition of marketing falls within one of the above three exceptions, an authorization will not be required because the communication will most likely be for treatment or health care operations purposes.

The HITECH Act adds another layer that must be considered to determine if a communication is marketing. It specifies that a communication about a product or service that encourages recipients of the communication to purchase or use that product or service is not a health care operations function unless it meets one of the three exceptions to the definition of marketing in HIPAA and does not involve direct or indirect payment for making such communication. However, even if payment is involved, such a communication will not be considered marketing if the communication is for treatment purposes, or if:

- The communication only describes a drug or biologic that has been previously prescribed or administered, provided the amount of the payment is reasonable
- A covered entity makes the communication pursuant to an authorization from the recipient of the communication
- A business associate makes the communication pursuant to its business associate agreement

These requirements become effective 12 months after enactment of the HITECH Act.

Access to EHR
HIPAA currently requires covered entities to provide individuals with a copy of their PHI in the form or format requested by the individual, only if it is readily producible in such form or format. The HITECH Act now provides individuals with the right to obtain a copy of their PHI in an electronic format (E-PHI) from a covered entity that uses or maintains an EHR. The HITECH Act also permits individuals to designate another person or entity to be the recipient of the transmittal of such E-PHI. HIPAA currently does not permit such designation, and the individual would have to sign an authorization. The HITECH Act prohibits covered entities from imposing a fee that exceeds the labor costs for responding to these types of requests.

The requirements become effective 12 months after enactment of the HITECH Act.

Opt-Out of Fundraising Communications
HIPAA currently requires covered entities to include "opt-out" language (i.e., instructions on how to opt-out of receiving future such communications) to be included with fundraising communications. The HITECH Act requires such opt-out language to be clear and conspicuous, but does not define what is considered to be "clear and conspicuous."

Currently, HIPAA only requires covered entities to take "reasonable efforts" to not send further fundraising communications to those who opt-out. The HITECH Act requires that covered entities must treat any opt-out as a revocation of authorization.

These requirements become effective 12 months after enactment of the HITECH Act.

Preemption of State Laws
The HITECH Act does not change the current HIPAA preemption rules. State laws that are more protective of patient privacy will not be preempted by HIPAA and will continue to apply.

Education on Health Information Privacy and Further Governmental Studies and Guidance
Within 12 months, the OCR is required to "develop and maintain a multi-faceted national educational initiative to enhance public transparency" regarding uses of PHI.

The HITECH Act requires HHS to conduct a number of studies related to privacy and security, including complaints, application of the rules to entities that are not covered entities or business associates (e.g., personal health record vendors), de-identification of data, and the definition of psychotherapy notes.

Legal News Alert is part of our ongoing commitment to providing up-to-the-minute information about pressing concerns or industry issues affecting our health care clients and colleagues. If you have any questions about this alert or would like to discuss this topic further, please contact your Foley attorney or any of the following individuals:

Lisa J. Acevedo
Chicago, Illinois
312.832.4381
lacevedo@foley.com

Jennifer L. Rathburn
Milwaukee, Wisconsin
414.297.5864
jrathburn@foley.com

Shirley P. Morrigan
Los Angeles, California
213.972.4668
smorrigan@foley.com

Michael Scarano
San Diego/Del Mar, California
858.847.6712
mscarano@foley.com

ABOUT FOLEY

Foley & Lardner LLP is a national law firm providing comprehensive legal services for innovative enterprises in the health care, pharmaceutical, biotechnology, and biomedical sectors. Our Health Care attorneys provide counsel on financial transactions, mergers, acquisitions, affiliations, joint ventures, regulatory and government compliance, and business operations. With offices throughout the United States and the backing of Foley's Health Care Industry Team — consistently ranked as one of the top health care law firms nationally and regionally by *Chambers USA* — Foley is well-positioned to serve the wide-ranging needs of health care entities across the country.

Foley & Lardner LLP Legal News Alert is intended to provide information (not advice) about important new legislation or legal developments. The great number of legal developments does not permit the issuing of an update for each one, nor does it allow the issuing of a follow-up on all subsequent developments.

If you do not want to receive further Legal News Alert bulletins, please e-mail info@foley.com or contact Marketing at Foley & Lardner LLP, 321 N. Clark Street, Suite 2800, Chicago, IL 60654 or 312.832.4500.