

Major Changes to HIPAA Security and Privacy Rules Enacted in Economic Stimulus Package

By Ross C. D'Emanuele, John T. Soshnik, and Kari Bomash, Dorsey & Whitney LLP
Minneapolis, MN

The HITECH Act is the largest and most consequential expansion and change to the federal privacy and security rules since the beginning of the HIPAA privacy and security programs.

President Obama signed into law on February 17, 2009 a \$787 billion economic stimulus package.¹ The stimulus package includes the Health Information Technology for Economic and Clinical Health Act, or "HITECH Act."

The HITECH Act is the largest and most consequential expansion and change to the federal privacy and security rules² since the beginning of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security programs. A major portion of the HITECH Act creates new federal privacy and security provisions that will have significant operational and legal consequences for healthcare providers, health plans, healthcare clearinghouses, their "business associates," and some vendors and service providers

that were not previously considered "business associates." This article summarizes the privacy and security provisions of the HITECH Act, and explores their impact on healthcare providers, health plans, and their business associates.

I. SECURITY PROVISIONS

A. Technical Safeguards Guidance
Currently, the HIPAA security regulations do not mandate use of any particular technical system or safeguards. The HITECH Act changes this, to a degree. The Department of Health and Human Services (HHS) must issue guidance annually on the "most effective and appropriate technical safeguards for use in carrying out" the HIPAA security standards.

Although the statute does not state that the technical safeguards

set forth in HHS guidance are the *only* effective and appropriate technical means of satisfying HIPAA security safeguards, they are the "most effective and appropriate" means of security compliance. Those covered entities and business associates who choose not to comply with the HHS guidance should justify their choice of technical systems that are not the most effective and appropriate means of compliance.

B. Breach Notification Requirements
For the first time, HIPAA covered entities will be required to provide specific notification to individuals if they discover a breach of unsecured protected health information (PHI). Written notification to individuals must be provided by first-class mail, and if the covered entity lacks sufficient contact information for 10 or more individuals, notification must also be made on the home page of the covered entity's website, or in major print or broadcast media. If the breach involves more than 500 residents of a state or jurisdiction, then notification also must be made to prominent media outlets in that state or jurisdiction.

The notification must be made within 60 calendar days after discovery, and must contain among other things: (1) a brief description of what happened, including the date of the breach (if known), and the date of discovery; (2) the steps the individual should take to protect themselves from potential harm resulting from the breach; and (3) a brief description of what the covered entity is doing to investigate the breach, to mitigate losses, and to protect against further breaches.

A “discovery” of a breach occurs not only when the covered entity or business associate knows of the breach, but also when the breach should reasonably have been known to the covered entity or business associate.

Covered entities must provide notice to HHS of all breaches. If the breach involves 500 or more persons, notice to HHS must occur immediately. Covered entities are permitted to keep a log of breaches involving less than 500 individuals, and submit the log annually to HHS.

The entire breach notification process applies only to “unsecured protected health information,” which means PHI that is not secured through a technology or methodology that HHS has stated renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals. The HITECH Act required the HHS Secretary to issue guidance within 60 days after enactment specifying the technologies and methodologies that satisfy this requirement. The Secretary issued the guidance on April 17, 2009, which stated that PHI secured through encryption or destruction in accordance with specified standards would not be unsecured PHI.³

If a healthcare provider or health plan utilizes the technologies and methodologies that HHS prescribes, then the PHI is not

The new statute tightens restrictions on use of PHI for marketing purposes.

“unsecured protected health information,” and none of the breach notification provisions apply to a breach of that information. This is a tremendous incentive for healthcare providers and health plans to use technologies and methodologies that HHS prescribes, in order to avoid the expensive breach notification requirements, including reporting breaches to HHS.

Business associates of HIPAA covered entities must report breaches to their covered entities, including the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

HHS must promulgate interim final regulations to implement all of the breach notification provisions within 180 days after enactment of the HITECH Act, and the breach notification provisions become effective 30 days after publication of such regulations.

II. PRIVACY PROVISIONS

A. Minimum Necessary Restrictions
The current HIPAA privacy regulations state that, with a few exceptions (such as for treatment purposes), a covered entity that uses, discloses, or requests PHI must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose.⁴

There is no current definition of “minimum necessary.” The HITECH Act changes that. Now, a covered entity is treated as in compliance with the minimum necessary standard only if the covered entity limits PHI, to the

extent practicable, to the “limited data set” as currently defined in the HIPAA privacy regulations. A “limited data set” is information that excludes names, postal address (other than city, state, and zip code), telephone and fax numbers, email address, social security and medical record numbers, and nine other identifiers.⁵

In other words, the limited data set is now essentially a safe harbor of compliance with the minimum necessary standard. If covered entities wish to use more than the limited data set, they should be prepared to justify why use of the limited data set is not practicable.

HHS must publish guidance on what constitutes “minimum necessary” under the privacy rules. On the date that such guidance is issued, the provisions noted above designating the limited data set as a minimum necessary safe harbor no longer apply.

B. Disclosure Accounting Expanded
Current HIPAA privacy rules grant individuals the right to receive from a covered entity information about the disclosures of PHI regarding the individual that the covered entity has made.⁶ There are certain disclosures that a covered entity need not include in this disclosure listing (called an “accounting of disclosures”), the largest and most important of which are all disclosures for treatment, payment, and healthcare operations.

The HITECH Act eliminates this exception from the disclosure accounting rules for covered entities and business associates that use or maintain an electronic health record. Entities that use or maintain an electronic health record must provide an accounting of disclosures for treatment, payment, and healthcare operations, in addition to all other disclosures that must be accounted for.

One of the most consequential changes in the HITECH Act is the extension of many HIPAA security and privacy rules to “business associates” of HITPAA covered entities.

HHS must promulgate new regulations setting out what information must be collected about these treatment, payment, and healthcare operations disclosures within six months of guidance on recommended technologies that will facilitate such disclosures from the Health Information Technology Policy Committee, a new advisory body created under the HITECH Act.

If a covered entity acquired an electronic health record as of January 1, 2009, the new disclosure accounting rules apply to disclosures made on and after January 1, 2014. If a covered entity acquires an electronic health record after January 1, 2009, the rules apply to disclosures made on or after the later of January 1, 2011 or the date the covered entity acquires the electronic health record system. HHS is permitted to delay both of these effective dates for up to two years.

An “electronic health record” is defined as an “electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.” This definition will likely require some additional guidance from HHS, because it is unlikely that physicians and other clinical staff would perform all of the described functions of creating, gathering, managing,

and consulting a typical electronic health record system.

Covered entities have the option of providing an accounting of all disclosures that the covered entity makes and that all of the covered entity’s business associates make; or they may make the accounting for all of the covered entity’s disclosures only, and provide the patient with a list of all business associates (including contact information), so that the patient may request an accounting from the business associates directly.

This is a significant new burden on business associates. The statute suggests that a business associate that does not use an electronic health record would not need to account for treatment, payment, and healthcare operations disclosures, but that point is not clear and will hopefully be a topic of future guidance.

C. Restriction Requests Mandatory

Under current HIPAA rules, an individual has the right to request restrictions on use and disclosure of PHI about the individual for treatment, payment, and healthcare operations beyond what HIPAA requires.⁷ However, a covered entity is not required to agree to such requests.

Now, under the HITECH Act provisions, covered entities must agree to requested restrictions on disclosures of PHI about an individual if the disclosure is to a health plan for purposes of carrying out payment or healthcare operations (and is not for treatment purposes), and the PHI pertains solely to a healthcare item or service for which the healthcare provider involved was paid out of pocket in full.

In other words, as a general rule, if a patient pays for a service out of pocket, then the patient is

permitted to demand that information regarding the service not be disclosed to the patient’s health plan or insurance. Failing to comply with this patient demand would be a violation subject to HIPAA penalties.

D. Prohibition on Sale of Records

The HITECH Act adds new provisions that prohibit a covered entity or business associate from directly or indirectly receiving payment in exchange for any PHI, unless the individual who is the subject of the PHI signs a written authorization specifically stating that the PHI can be exchanged for payment.

There are a few exceptions to this general prohibition of exchanging payment for PHI, among which are exchanges for treatment purposes; for purposes of a sale, transfer, merger, or consolidation of covered entities; and for research purposes (so long as the price reflects only the costs of preparation and transmittal of the data).

Regulations to implement these sale prohibitions must be promulgated within 18 months of enactment, and the provisions apply to exchanges that occur six months following promulgation of the regulations.

E. Patient Access to Electronic Health Records

If a covered entity uses or maintains an electronic health record, then individuals have a right to receive a copy of the PHI maintained in the electronic health record in an electronic format. Fees that a covered entity wishes to charge for providing the records may be no greater than the labor costs incurred to respond to the request.

F. Marketing Communications

The new statute tightens restric-

tions on use of PHI for marketing purposes. First, covered entities may not treat communications that are “marketing” under the current regulations⁸ (and therefore require written patient authorization for use and disclosure) as also “health-care operations” (and therefore permitted without authorization).

In addition, communications that fall within the current exceptions to the marketing definition are nonetheless not allowed under the HITECH Act if the covered entity is paid to make the communication, unless either: (1) the communication describes only a drug or biologic that is currently prescribed for the patient and the payment the covered entity receives is reasonable; (2) the covered entity itself makes the communication and obtains a written patient authorization; or (3) a business associate makes the communication, and the communication is consistent with the business associate agreement between the covered entity and the business associate.

These marketing rules apply to all communications made on or after February 17, 2010.

G. *Opt-Out Requirement for Fundraising Communications*

All fundraising communications that are considered healthcare operations must provide, in a clear and conspicuous manner, an opportunity for the recipient to elect not to receive any further such communications. This is similar to the current HIPAA regulations on fundraising communication,⁹ and this new statute appears directed at covered entities who may have treated their fundraising as part of “healthcare operations” to avoid the opt-out requirement under current law. This provision is effective for all communications occurring on or after February 17, 2010.

The HITECH Act substantially increases the magnitude of HIPAA enforcement risk . . .

III. IMPACT ON BUSINESS ASSOCIATES

A. *Security Standards Applicable to Business Associates*

One of the most consequential changes in the HITECH Act is the extension of many HIPAA security and privacy rules to “business associates” of HIPAA covered entities. Under previous law, business associates were required (pursuant to their business associate agreements with covered entities) to implement administrative, physical, and technical safeguards that “reasonably and appropriately” protect PHI.¹⁰ Business associates were liable for a breach of such security obligations only under the business associate agreements, and were not directly subject to HIPAA enforcement. The HITECH Act states that all of the HIPAA security administrative safeguards, physical safeguards, technical safeguards, and security policies, procedures, and documentation requirements apply directly to all business associates. This means that HHS (and state attorneys general under the new enforcement provisions) may impose fines directly against business associates of HIPAA covered entities who do not comply with these HIPAA security standards. This will likely increase the cost and legal risks of being a business associate to a HIPAA covered entity.

In addition, these new business associate security requirements must be added to all business associate agreements.

All additional requirements in the HITECH Act that relate to security and that are applicable to covered entities also are applicable to business associates and must be incorporated into business associate agreements. All civil and criminal penalties applicable to covered entities for violating the security provisions are also applicable to business associates.

B. *Privacy Provisions and Business Associates*

Similarly, the HITECH Act makes certain privacy provisions directly applicable to business associates. A business associate may use and disclose PHI only if such use or disclosure is in compliance with all business associate agreement requirements. Therefore, if a business associate uses or discloses PHI in violation of the privacy obligations in its business associate agreement with a covered entity, the business associate is not only liable to the covered entity under the business associate agreement, but also is directly liable to HHS for the same noncompliant use or disclosure.

All other privacy provisions in the HITECH Act are applicable to business associates and must be added to business associate agreements. Again, a business associate will be liable for breach to the covered entity to the extent applicable in a business associate agreement, and directly liable to HHS (or state attorneys general) for failure to comply with the additional privacy requirements set forth above.

Business associates also must take action if they know of a pattern of activity or practice of the business associate that constitutes a material breach or violation of a business associate agreement. If the business associate fails to take reasonable steps to cure the

breach, terminate the agreement, or report the problem to the HHS, then the business associate may be liable under HIPAA penalties, including the new civil monetary penalty (CMP) tiers described below.

C. *Other Business Associate Requirements*

As noted above, the HITECH Act requires business associates to notify applicable covered entities of breaches of unsecured PHI. The HITECH Act provisions on marketing communications, minimum necessary standards, prohibitions on sale of PHI, accounting of disclosures to individuals, and audit provisions all apply directly to business associates as described above. And if a business associate fails to comply with these new provisions, then penalties can be imposed on the business associate just as penalties can be imposed on covered entities.

D. *Entities Considered Business Associates*

Certain organizations (such as health information exchange organizations and regional health information organizations) are required to enter into a business associate agreement and are treated as business associates under the HITECH Act if they: (1) provide data transmission of PHI to a covered entity (or its business associate) and require access on a routine basis to such PHI; or (2) contract with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record. However, the statute states these organizations are business associates only for purposes of the privacy subtitle of the HITECH Act and the current HIPAA privacy and security regulation, which may indicate that these organizations are not to be treated

as business associates for any new HIPAA privacy and security regulations promulgated in the future.

IV. VENDORS OF PERSONAL HEALTH RECORDS AND OTHER NON-HIPAA ENTITIES

In addition to new breach notification provisions applicable to covered entities and business associates, the HITECH Act adds temporary breach notification requirements applicable to vendors of personal health records and other non-covered entities and non-business associate entities that interact with personal health records. A “personal health record” is an electronic record of certain identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. These provisions appear directed at patient-directed health record programs, some of which currently fall outside of HIPAA regulation.

Each vendor of personal health records, following the discovery of a “breach of security” of unsecured identifiable health information that is in a personal health record maintained and offered by such vendor, must notify each individual who is a citizen or resident of the U.S. whose unsecured identifiable health information was acquired by an unauthorized person as a result of such breach of security, and notify the Federal Trade Commission (FTC) as well. This notification requirement also applies to: (1) entities that offer products or services through the website of a vendor of personal health records; (2) entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals personal health records; and (3) entities that are not covered

entities and that access information in a personal health record or send information to a personal health record, if the breach of security of unsecured identifiable health information is through a product or service provided by such entity.

Third-party service providers that furnish services to vendors of personal health records or to the other entities in connection with the offering or maintenance of a personal health record or related product or service must notify the vendor or entity of a breach of security that results from such services. This notification must identify each individual whose unsecured identifiable health information has been or is reasonably believed to have been accessed, acquired, or disclosed during such breach.

The specific breach notification content and process requirements that apply to covered entities and business associates also are applicable to notifications related to personal health records. The HITECH Act required the FTC to promulgate interim final regulations no later than 180 days after the enactment date to implement these provisions, and they apply to breaches of security discovered on or after 30 days after promulgation of such regulations. The FTC issued a proposed rule on breach notification on April 16, 2009.¹¹

Violations of the notification requirements applicable to vendors of personal health records and the entities and third-party service providers described above are treated as unfair and deceptive acts or practices in violation of the Federal Trade Commission Act.

V. NEW ENFORCEMENT PROVISIONS

The HITECH Act substantially increases the magnitude of HIPAA enforcement risk through: (1) increasing the CMP and civil settle-

ment amounts; (2) adding provisions on willful neglect violations; and (3) allowing state attorneys general to enforce HIPAA privacy and security violations.

A. *New Civil Monetary Penalty System*

The HITECH Act creates a new tiered CMP system in which the CMP amount is tied to the violator's level of intent. If the violator "did not know (and by exercising reasonable due diligence would not have known)" of the violation, then the range of possible penalties is a minimum of \$100 per violation, but not more than \$25,000 for violations of the same requirement in a calendar year. Violations due to "reasonable cause" and not "willful neglect" have a CMP minimum of \$1,000 per violation, but no more than \$50,000 for violations of the same requirement in a calendar year. In both cases the maximum range of CMP is \$50,000 per violation, but no more than \$1,500,000 for violations of the same requirement in a calendar year.

For violations committed with willful neglect, the legislation creates two categories of CMPs. If the willful neglect violation is corrected within 30 days of the date the violator knew or should have known of the violation, the CMP range is a minimum of \$10,000 per violation, but no more than \$250,000 for violations of the same requirement in a calendar year and a maximum of \$50,000 per violation, but no more than \$1,500,000 for violations of the same requirement in a calendar year. If the willful neglect violation is not corrected, the minimum violation is \$50,000 per violation with no maximum penalty. Within the lawful ranges HHS is to determine the CMP based on the nature and extent of the violation and the harm caused to individuals.

[T]he most general and long term impact of the HITECH Act may be to increase privacy and security as a compliance priority.

The new level of CMPs applies immediately to all violations.

HHS will use the CMP proceeds to enforce the HIPAA privacy and security standards. Within three years of enactment, HHS must promulgate a regulation to distribute a portion of CMP proceeds directly to harmed individuals. This will provide an incentive for individuals to report alleged violations to HHS and state attorneys general.

B. *Willful Neglect*

In addition to the new CMP tiers, the statute mandates that HHS investigate complaints if a preliminary investigation indicates that the violation may have been due to willful neglect. If HHS finds that a violation is due to willful neglect, HHS must impose a penalty on the violator. HHS must promulgate regulations to implement these willful neglect provisions within 18 months of enactment, and the provisions apply to penalties imposed on or after February 17, 2011.

C. *State Attorney General Actions*

Potentially more problematic for covered entities and business associates than the increased CMPs, the HITECH Act allows state attorneys general to enforce violations of the HIPAA privacy and security rules against covered entities and business associates if: (1) they have not

Examine Diagnose Treat Cure

That's what physicians do for their patients and that's what they expect from you when their symptoms point to internal compliance problems.

We work in collaboration with you to examine, diagnose, treat and cure clients' billing, coding, claims, medical records and compliance practices. VantagePoint consultants help investigate, understand and defend allegations of abusive or fraudulent billing or compliance issues. Our certified coders and clinical nurse reviewers can provide you with in-depth expertise when conducting reviews for healthcare clients.

- Compliance Risk Assessments
- Claims Reviews & Analysis
- Auditing of Medicare & Medicaid reviews
- DRG Validation



VantagePoint

Strategic, Financial & Compliance
Solutions for Healthcare

9 Washington Avenue
Hamden, Connecticut 06518
www.vantagepointconsult.com
info@vantagepointconsult.com
PH: 203.288.6860

been corrected in 30 days; and (2) the violation threatens or adversely affects one or more of the state's residents. An attorney general can either enjoin the violator or may obtain damages equal \$100 per violation up to \$25,000 for violations of the same requirement in a calendar year. A court may award attorney fees and the costs of the action to the state.

D. Audit Authority

HHS is provided additional authority to audit covered entities and business associates to ensure compliance with the privacy portion of the HITECH Act and the current HIPAA privacy and security regulations. It is unclear whether Congress intended to ensure that this audit authority does not extend to the security portion of the HITECH Act or any HIPAA privacy and security rules that may be promulgated in the future, but certainly a technically accurate reading of the HITECH Act would limit the audit authority in this manner.

VI. CONCLUSION

The immediate impact of the HITECH Act on covered entities is significant. First, covered entities must consider whether all of their uses, disclosures, and requests for PHI are in compliance with the "minimum necessary" standard, now that a limited data set has been defined as compliance with that standard.

Second, all business associate contracts must be amended to include the additional provisions now applicable to business associates.

Lastly, covered entities must consider whether and how changes to the marketing, fundraising, and restriction request rules affect their operations; and how the new

disclosure accounting and breach notification rules factor into their choices regarding health information systems and infrastructure.

For business associates the HITECH Act means even more dramatic changes. For the first time business associates have direct liability under HIPAA, and must directly comply with a host of administrative, technical, physical, and policy-related security rules. For some business associates this will mean implementation of a new information security program. For all business associates this will necessitate a thorough review of existing security safeguards, policies, and procedures to ensure compliance.

Business associates must anticipate significant amendments to their business associate agreements, and must also consider how they will comply with the host of new privacy and security rules that will now apply to them.

Finally, covered entities and business associates must remember that the HITECH Act significantly alters the entire HIPAA enforcement environment by increasing the penalties and eliminating in many situations enforcement discretion not to impose penalties. Accordingly, the most general and long term impact of the HITECH Act may be to increase privacy and security as a compliance priority.

Ross C. D'Emanuele is a partner in Dorsey's Health Group, and Chair of the Life Sciences and Health Care group. He counsels a wide variety of public, private, nonprofit and for-profit entities in the healthcare field, with specific emphasis on healthcare fraud and abuse, credentialing and medical and pharmacy practice act matters, food and drug law, and privacy regulation, including Medicare/Medicaid and private payor reimbursement, corporate

compliance programs, drug and medical device approval and post-market regulatory matters, and technology transfer and clinical trials.

A Partner in the Health Group at Dorsey, John Soshnik has developed a well-rounded health law practice, focusing on transactions and regulatory issues for healthcare providers, healthcare benefit companies, and managed care organizations. Mr. Soshnik has also developed specialized knowledge regarding the integration of healthcare benefits and financial solutions (including consumer-driven healthcare products such as health savings accounts, coordinated investment products and credit products), health data and financial information privacy (including HIPAA, Gramm-Leach-Bliley, and other state and federal privacy law), healthcare fraud and abuse, and related regulatory and compliance issues.

Kari Bomash is a member of Dorsey's Health Transactions and Regulations Practice Group. She is located in the firm's Minneapolis, MN office.

- 1 The American Recovery and Reinvestment Act, Pub. L. No. 111-5.
- 2 45 C.F.R. §§ 160, 164.
- 3 74 Fed. Reg. 19006 (Apr. 27, 2009).
- 4 45 C.F.R. §§ 164.502(b), 164.514(d).
- 5 45 C.F.R. § 164.514(e).
- 6 45 C.F.R. § 164.528.
- 7 45 C.F.R. § 164.522(a).
- 8 45 C.F.R. §§ 164.501; 164.508(a)(3).
- 9 45 C.F.R. §§ 164.514(f); 164.520(b)(1)(iii)(B).
- 10 45 C.F.R. § 164.314(a).
- 11 74 Fed. Reg. 17914 (Apr. 20, 2009).