



BNA's

HEALTH LAW REPORTER



Reproduced with permission from BNA's Health Law Reporter, 18 HLR 308, 03/05/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

ARRA 2009 and the HITECH Act: The Next Phase of HIPAA Regulation and Enforcement Arrives

BY REECE HIRSCH AND
REBECCA FAYED

On Feb. 17, when President Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA), it marked the beginning of a new phase in the evolution of federal law governing the privacy and security of medical information.¹ Title XIII of ARRA, the Health Information Technology for Economic and Clinical Health Act (the HITECH Act),² contains the most significant changes with respect to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) since the issuance of the final implementing privacy and security regulations (respectively, the Privacy Rule and the Security Rule).

As part of its effort to develop a nationwide health information technology infrastructure that allows for the electronic exchange of protected health information (PHI), Congress has, in Subtitle D of the HITECH Act, (1) extended the reach of HIPAA, the Privacy Rule and

the Security Rule, (2) imposed breach notification requirements on HIPAA covered entities and their business associates, (3) limited certain uses and disclosures of PHI, (4) increased individuals' rights with respect to PHI and, significantly, (5) increased enforcement of, and penalties for, violations of privacy and security of PHI. Many of the HITECH Act's provisions will be effective on Feb. 17, 2010 (12 months after its enactment), while other provisions require regulations to be implemented or may become effective two years or more after the law's enactment.

Bills seeking to amend the Privacy Rule and Security Rule have been considered in Congress for the past few years, but were mired in debates between privacy advocates and health care industry groups. So why is now the time for sweeping new health care privacy and security laws? For the answer to that question, it's helpful to revisit the origins of HIPAA.

When the "administrative simplification" provisions in Title II of HIPAA were first enacted, the focus was on standardizing the formats for certain electronic transactions, thus creating efficiencies and moving the industry away from paper claim forms. For many in the health care industry, the HIPAA privacy and security provisions seemed to be almost an afterthought, premised upon the assumption that as more medical information was transmitted electronically using the new standard transactions, risks to the privacy and security of that data would increase. In the HITECH Act, the effort to create savings by streamlining the flow of information within the health care industry (this time in the form of electronic health records, personal health records and health information exchanges) has once

¹ American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009) (ARRA).

² ARRA at § 13001(a).

Reece Hirsch is a partner in the San Francisco office of Sonnenschein Nath & Rosenthal LLP, and can be reached at (415) 882-5040 or rhirsch@sonnenschein.com. Rebecca Fayed is an associate in Sonnenschein's Washington office, and can be reached at (202) 408-6351 or rcfayed@sonnenschein.com.

again led to new privacy and security measures intended to keep pace with new risks to data.

Breach Notification

The HITECH Act's security breach notification provisions are reflective of a movement to protect consumers from the fallout of privacy and security breaches that got its impetus in the wake of a major incident involving ChoicePoint Inc. in 2005. Since 2005, most states have passed security breach notification laws, and there have been repeated efforts to pass a federal security breach notification law. While federal security breach notification bills of general applicability have stalled in Congress due in part to committee turf wars and debates among privacy advocates and business groups about a few key provisions, such as preemption of state law, the HITECH Act sets rigorous new standards for breach notification in the health care industry.

- **Breach Notification Requirement.** The HITECH Act requires covered entities to notify individuals whose "unsecured PHI" has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a breach.³ Unlike many state security breach notification statutes, the HITECH Act applies to breaches involving both electronic and paper records.
- **Definition of Breach.** A "breach" is defined as the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom the information is disclosed "would not reasonably have been able to retain such information."⁴ The meaning of that last phrase is a bit ambiguous, but it could apply to a situation in which a laptop containing PHI is stolen, but recovered almost immediately without any real opportunity for the thief to extract the PHI. A breach does not include unintentional access to PHI by an employee or other individual acting under the authority of a covered entity or business associate if (1) the access was made in good faith and within the scope of employment or other professional relationship and (2) the information was not further acquired, accessed, used, or disclosed by any person. A breach also does not include an inadvertent disclosure from an individual authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility, provided that the information is not further acquired, accessed, used, or disclosed by any person.⁵
- **Business Associates.** Business associates must notify covered entities of any breach of which they become aware.⁶ It is important to note that business associates are not required to notify affected individuals of a breach, but may fulfill their legal obligations by notifying the covered entity of the breach.

- **Unsecured PHI Guidance.** Within 60 days of enactment of the HITECH Act (i.e., by April 17), the secretary of the Department of Health and Human Services (HHS) is required to issue (and annually update) guidance on what constitutes "unsecured PHI" that may trigger notification duties in the event of a breach.⁷ If HHS does not issue guidance in accordance with the timeline, a default provision will apply, and unsecured PHI will be defined as any PHI that is not secured by a technology standard (such as encryption) accredited by the American National Standards Institute that renders the information unusable, unreadable or indecipherable.⁸ Because the breach notification requirement applies to PHI in all forms, presumably this HHS guidance would address appropriate methods for shredding documents, wiping hard drives prior to disposal, and encryption. In addition, HHS must issue annual guidance on appropriate encryption methods and similar technologies.⁹
- **Timing of Notice.** Notification of a breach must be made "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach."¹⁰ Covered entities will have the burden of demonstrating that a notification meets this timing requirement, including presenting evidence to support the necessity of any delay.¹¹ A breach is deemed to be "discovered" as of the first day that the breach is known, or reasonably should have been known, to the covered entity or its business associate.¹² The knowledge of any employee, officer or agent (other than the person committing the breach) will be imputed to the organization for purposes of establishing discovery and starting the clock running.¹³
- **Individual Notice.** Notification to the individual must be made in writing and sent to the individual via first class mail unless the individual has specified a preference for electronic mail.¹⁴ If the covered entity has insufficient or out-of-date contact information, the covered entity must give notice in a substitute form, including posting notice of the breach on its Web site or in major print or broadcast media (if the covered entity has insufficient information for more than 10 individuals affected).¹⁵
- **Media Notice.** If the breach involves the PHI of more than 500 individuals in a state, the covered entity must give notice of the breach to prominent media outlets in that state.¹⁶ If a covered entity is able to notify all affected individuals of such a breach, then it would seem that this media notice requirement is primarily punitive in intent.
- **HHS Notice.** Covered entities must notify HHS of any breach. If the disclosure involves the PHI of more than 500 individuals, HHS must be notified immediately. If fewer than 500 individuals are af-

³ ARRA at § 13402(a).

⁴ ARRA at § 13400(1)(A).

⁵ ARRA at § 13400(1)(B). There appears to be a drafting error in this provision, but the sentence to which this footnote is appended reflects what we believe is the intended meaning. It appears that Sections 13400(1)(B)(ii) and 13400(1)(B)(iii) should properly be linked as elements of a single exception to the definition of "breach."

⁶ ARRA at § 13402(b).

⁷ ARRA at § 13402(h)(2).

⁸ ARRA at § 13402(h)(1)(B).

⁹ ARRA at § 13402(h)(2).

¹⁰ ARRA at § 13402(d)(1).

¹¹ ARRA at § 13402(d)(2).

¹² ARRA at § 13402(c).

¹³ ARRA at § 1340(c).

¹⁴ ARRA at § 13402(e)(1)(A).

¹⁵ ARRA at § 13402(e)(1)(B).

¹⁶ ARRA at § 13402(e)(2).

ected, the covered entity may maintain a log to be produced to HHS annually.¹⁷

- **Content of Notice.** Notice of a breach must include a description of the facts surrounding the breach, the type of PHI involved, the steps individuals should take to protect themselves, what the covered entity is doing to investigate, mitigate and protect against future breaches, and contact information for individuals to ask questions or obtain more information.¹⁸
- **Report to Congress on Breaches.** By Feb. 17, 2010, and annually thereafter, HHS is required to submit a report to the Senate and House regarding the number of and nature of breaches reported to HHS and actions taken in response to such breaches.¹⁹
- **Effective Date.** HHS is required to issue interim final regulations on the HITECH Act's breach notification provisions no later than 180 days after enactment. The new breach notification provisions will become effective for breaches discovered 30 days after the publication of the interim final regulations.²⁰

The HIPAA Privacy and Security Rules do not currently require covered entities to notify individuals when their PHI has been subject to a breach. State breach notification laws generally require notification of individuals whose financial information (such as Social Security number or credit card number) has been subject to unauthorized access. The HITECH Act adds more detailed and stringent provisions to many of the common elements of state security breach notification laws, such as the act's requirements regarding (1) the content of the notice, (2) media notice, (3) acceptable encryption technologies, and (4) the 60-day deadline for notification. Applying security breach notification standards to medical information is consistent with concerns expressed by the Federal Trade Commission (FTC) and other regulators about the growing crime of medical identity theft.

For covered entities, the HITECH Act's security breach notification provisions largely will supersede compliance with existing state notification laws, given the very broad definition of PHI and the HITECH Act's detailed and stringent notification requirements. However, certain more stringent state notification requirements will not be preempted by the HITECH Act, such as state laws that require notification to certain state agencies in the event of a breach.

New Regulation of Personal Health Record Vendors

The recent movement to adopt personal health records (PHRs), spurred by the efforts of large employers, has led to concerns that vendors of PHR products are not necessarily required by law to report breaches involving PHR data. Most state security breach notification laws do not define "personal information" to include medical information, focusing instead on information that may be used to commit financial fraud. The HITECH Act addresses that perceived deficiency by extending the security breach notification provisions de-

scribed above to (1) PHR vendors, (2) businesses that offer products or services through a Web site of a PHR vendor or a covered entity that offers PHRs, and (3) entities that access information in, or send information to, a PHR (collectively, PHR businesses).

- **Notification of PHR Breach.** Because PHR businesses are not covered entities under HIPAA subject to regulation by HHS, the HITECH Act provides for regulation of such businesses by the FTC. PHR businesses are required to notify the FTC and each affected individual who is a citizen or resident of the United States of a privacy or security breach of unsecured individually identifiable information in a PHR (PHR information).²¹ If a PHR vendor utilizes the services of a third-party service provider in performing the PHR service, then that service provider must notify the PHR vendor of any breach upon its discovery.²² The FTC will notify HHS upon receiving notice of a PHR breach.²³ This collaborative enforcement approach was previewed in January when HHS and the FTC simultaneously announced settlements with CVS Pharmacy Inc. arising from a security breach incident.
- **FTC Regulatory Authority.** The FTC will have the authority to take action against violations of the notification requirements related to PHR information as unfair and deceptive acts or practices under the Federal Trade Commission Act.²⁴
- **Effective Date.** The FTC must issue interim final regulations regarding PHR breach notification requirements within 180 days from the enactment of the HITECH Act. The new breach notification requirements will apply to breaches that are discovered on or after 30 days from the publication of the FTC's interim final regulations.²⁵

Business Associates—Increased Duties and Penalties

Prior to the enactment of the HITECH Act, HIPAA applied to business associates only indirectly by way of the business associate's contractual obligations to the covered entity. Similarly, the penalty for a violation of these obligations was merely damages that resulted from any contractual breach (unless the business associate also happened to be a covered entity). The HITECH Act, however, has expanded both the application of HIPAA requirements and penalties to business associates. The imposition of these new requirements reflects a concern that a wide range of businesses are now involved in the transmission, processing and storage of PHI, but are not directly regulated under HIPAA. Because the entities subject to regulation under HIPAA (health care providers, health plans, and health care clearinghouses) was defined by the HIPAA statute, a statutory measure such as the HITECH Act was necessary to remedy this perceived deficiency.

- **Security Rule Obligations.** The HITECH Act requires business associates to comply with the Security Rule's administrative, technical, and physical safeguard requirements and requires business associates to implement security policies and pro-

¹⁷ ARRA at § 13402(e)(3).

¹⁸ ARRA at § 13402(f).

¹⁹ ARRA at § 13402(i).

²⁰ ARRA at § 13402(j).

²¹ ARRA at § 13407(a).

²² ARRA at § 13407(b).

²³ ARRA at § 13407(d).

²⁴ ARRA at § 13407(e).

²⁵ ARRA at § 13407(g)(1).

cedures in the same manner as a covered entity.²⁶ If the business associate violates any of these Security Rule provisions, the business associate may be subject to the same HIPAA civil and criminal penalties as a covered entity.²⁷ For many vendors to the health care industry, this may be the provision of the HITECH Act with the greatest impact (and attendant costs). A business associate's new obligations under the Security Rule will include (1) implementing written policies and procedures that address each of the Security's Rule's administrative, technical, and physical safeguard standards, (2) implementing a security awareness and training program for workforce members, (3) designating a security official, and, (4) perhaps most significantly, conducting an "accurate and thorough" security risk analysis, coupled with a security management process. Large business associate organizations, such as application service providers and data storage companies, may already have implemented comprehensive security compliance programs that are consistent with Security Rule standards. However, for many smaller business associate organizations, and particularly those for which the health care industry represents only a part of their business, these new Security Rule obligations may require significant upgrades to existing data security compliance programs.

- **Privacy Rule Obligations.** While the HITECH Act makes certain Security Rule provisions directly applicable to business associates, it takes a less direct approach with respect to the Privacy Rule. Specifically, the HITECH Act requires the business associate to only use or disclose PHI consistent with its obligations under its business associate agreement with a covered entity (the provisions of which are dictated by the Privacy Rule).²⁸ The HITECH Act did, however, increase the potential liability for a business associate who breaches its contractual obligations.²⁹ That is, if a business associate violates the terms of its business associate agreement, the business associate may be subject to the same HIPAA civil and criminal penalties as a covered entity who violated the Privacy Rule.
- **Curing Breach of Business Associate Agreements.** Similar to the obligations currently imposed on covered entities, a business associate will be required to take reasonable steps to cure a breach of a business associate agreement or terminate the agreement if it knows of a pattern of activity or practice by a covered entity that violates the agreement.³⁰ If termination of the business associate agreement is not feasible, the business associate may be required to report the covered entity's compliance problem to HHS. However, it should be noted that a covered entity has far fewer contractual obligations than a business associate under a typical business associate agreement.
- **Organizations Transmitting PHI.** The HITECH Act clarifies that organizations that provide data transmission of PHI for covered entities and who re-

quire routine access to the PHI are business associates who must enter business associate agreements with the covered entities for whom they provide these services.³¹ The HITECH Act states that health information exchange organizations, regional health information organizations, e-prescribing gateways, and PHR vendors that provide a PHR to patients as part of a covered entity's electronic health record (EHR) are among the organizations that may be business associates under this provision.³² While many of these enumerated organizations already qualified as business associates under HIPAA, the HITECH Act seems intended to clarify that the exception for "conduit" organizations that are solely responsible for transmission of PHI should not exempt these enumerated organizations from business associate status.

- **Amendment of Business Associate Agreements.** The additional privacy and security requirements imposed upon business associates through the HITECH Act must be incorporated into the business associate agreement between the covered entity and the business associate.³³ Because large covered entity organizations may have hundreds of business associate agreements in place, amending those agreements could entail considerable administrative costs. The question of whether business associate agreements must be amended would benefit from further clarification from HHS, particularly in light of the fact that the new obligations are imposed upon business associates by force of law, rather than through required contract terms.
- **Obligation to Enter Into Business Associate Agreements.** Previously, the obligation to enter into a business associate agreement has rested squarely with the covered entity. Under the HITECH Act, it is unclear whether a business associate will be required to propose a business associate agreement when a covered entity has failed to do so. The HITECH Act provides that both the privacy- and security-related provisions described above "shall be incorporated into the business associate agreement between the business associate and the covered entity." Hopefully, future guidance from HHS will clarify whether that use of the word "shall" imposes a legal requirement on business associates to enter into business associate agreements.

Limitations on the Use and Disclosure of PHI

- **Marketing.**
 - The HITECH Act confirms the provision of the Privacy Rule that states that a communication by a covered entity about a product or service that encourages the recipient of the communication to purchase or use the product or service is not a marketing communication, but rather, a health care operation, if that communication is: (1) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication; (2) for treatment of that individual; or (3) for case management, care coordination or to recom-

²⁶ ARRA at § 13401(a).

²⁷ ARRA at § 13401(b).

²⁸ ARRA at § 13404(a).

²⁹ ARRA at § 13404(c).

³⁰ ARRA at § 13404(b).

³¹ ARRA at § 13408.

³² ARRA at § 13408.

³³ ARRA at § 13401(a) and 13404(a).

ment alternative treatments, therapies, health care providers, or settings of care to the individual.³⁴

- However, the HITECH Act limits this marketing exclusion by stating that, to the extent that the covered entity receives payment for making these communications, the communication is no longer a health care operation (and, presumably, is a marketing communication that requires an individual's authorization) *unless*: (1) the communication describes only a drug or biologic currently being prescribed for the individual and the amount of payment received for making the communication (if any) is reasonable in amount; (2) the communication is made by the covered entity and the covered entity has received a valid HIPAA authorization from the individual to whom it is making the communication; or (3) the communication is made by a business associate and is consistent with the terms of its business associate agreement with the covered entity.³⁵
- The exception for communications by a business associate in clause (3) above appears to be a product of imprecise and misleading drafting. As written, the provision seems to state that a covered entity could receive payment to make a communication that otherwise would require an individual's authorization, but would be exempt from the authorization requirement solely by virtue of the fact that the communication was made by a business associate acting on behalf of the covered entity, rather than directly by the covered entity. It appears that this provision may have been intended to provide instead that the fact that a business associate receives payment for making a communication in accordance with the terms of a business associate agreement does not constitute a receipt of payment that would trigger the HITECH Act's limitation on marketing communications.
- HHS will define the term "reasonable in amount" by regulation, but no time frame is mandated for the regulation.³⁶
- The following is an example of how the HITECH Act's limitation on marketing might be applied. A pharmaceutical company requests that a pharmacy covered entity distribute pamphlets describing a new cholesterol drug to pharmacy customers receiving a popular cholesterol medication. The pharmaceutical company will pay all costs associated with printing and distribution of the pamphlet. Under the current Privacy Rule, such a communication would probably be permitted without the patient's authorization as a communication by a covered entity to recommend alternative treatments or therapies. Under the HITECH Act, the communication probably would require the patient's authorization because the covered entity is receiving payment to make the communication and the communication does not describe a drug or biologic cur-

rently being prescribed for the individual, it describes an alternative drug.

- **Fund Raising.** The HITECH Act requires HHS to issue a rule that requires all written fund raising communications to provide the recipient with an opportunity to opt out of any future fund raising communications. Different from the Privacy Rule, the HITECH Act now requires covered entities to treat an individual's election to opt out of fund raising communications as a revocation of authorization.³⁷
- **Sale of EHRs or PHI.** The HITECH Act specifically prohibits the sale of EHRs or PHI by a covered entity or business associate without an individual's authorization unless the covered entity (or business associate) is receiving the remuneration for the EHRs or PHI for purposes of: (1) public health activities; (2) research, provided that the price charged reflects the costs of preparation and transmittal of data; (3) treatment; (4) the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity and the due diligence related to such activity; (5) providing a business associate with remuneration under a business associate agreement for services rendered; or (6) providing an individual with access to his or her PHI.³⁸
- **Minimum Necessary.**
 - The Privacy Rule requires covered entities to disclose only the minimum amount of PHI reasonably necessary to accomplish the purpose of the permitted use or disclosure of PHI (the "minimum necessary standard"). The minimum necessary standard has been criticized as one of the most vague and difficult-to-implement components of the Privacy Rule. The HITECH Act requires HHS to issue guidance on the minimum necessary standard within 18 months of the HITECH Act's enactment (*i.e.*, by Aug. 17, 2010).³⁹
 - For the period prior to the issuance of the secretary's minimum necessary guidance, the HITECH Act defines compliance with the minimum necessary standard as using or disclosing a limited data set, *to the extent practicable*, or if necessary, to the minimum necessary to accomplish the intended purpose of the use or disclosure.⁴⁰ The Privacy Rule defines a limited data set as data that is nearly de-identified (except that it may include dates and certain address information, such as city, state and ZIP code). It is likely that covered entities will often not find it practicable to utilize limited data sets for many common uses and disclosures of PHI for payment or health care operations purposes.
 - The Privacy Rule's exceptions to the minimum necessary standard (*e.g.*, treatment disclosures) remain in effect under the HITECH Act.⁴¹
 - The HITECH Act also requires HHS to issue guidance no later than 12 months after its enact-

³⁴ ARRA at § 13406(a)(1).

³⁵ ARRA at § 13406(a)(2).

³⁶ ARRA at § 13406(a)(3).

³⁷ ARRA at § 13406(b).

³⁸ ARRA at § 13405(d)(2).

³⁹ ARRA at § 13405(b)(1)(B).

⁴⁰ ARRA at § 13405(b)(1)(A).

⁴¹ ARRA at § 13405(b)(3).

ment on how best to implement the Privacy Rule's deidentification requirements.⁴²

- *Review of Health Care Operations.* While both the House and Senate bills required HHS to review the definition of health care operations and eliminate from the definition any activities that could reasonably and efficiently be conducted with deidentified health information or should require an authorization, the conference agreement that resulted in the final HITECH Act struck that provision. Thus, significantly, the HITECH Act *does not* require the secretary to review and modify the definition of health care operations.

Individual Rights

- *Accounting for Disclosures of PHI.*
 - The HITECH Act expands an individual's right to receive an accounting of disclosures of PHI, and thus, expands a covered entity's obligation with respect to accounting for disclosures.⁴³ While the Privacy Rule currently exempts from the accounting requirement those disclosures of PHI made for purposes of treatment, payment and health care operations, under the HITECH Act, if a covered entity uses or maintains an EHR, this exception does not apply to disclosures of that EHR.⁴⁴ It is our understanding that EHR products typically have the capability to maintain a record of disclosures of PHI outside the covered entity organization.
 - While the covered entity must account for disclosures of EHRs for purposes of treatment, payment and health care operations purposes under the HITECH Act, the reporting period for these disclosures is only for the three years prior to an individual's request for an accounting (instead of the six-year Privacy Rule requirement for all other disclosures).⁴⁵ This shortened time frame seems to recognize the added burden on covered entities of storing these additional EHR accounting records.
 - The HITECH Act also requires HHS to issue regulations regarding what information must be maintained about each disclosure of an EHR for purposes of treatment, payment or health care operations purposes.⁴⁶
 - The HITECH Act provides for a grace period for compliance with these new accounting requirements, including an extended grace period (until Jan. 1, 2014) for those covered entities who began using EHRs prior to Jan. 1, 2009.⁴⁷ For those covered entities who acquire an EHR after Jan. 1, 2009, the new accounting requirements apply to disclosures made on or after the later of January 1, 2011 or the date that the covered entity acquired the EHR.⁴⁸
- *Restrictions on Disclosures of PHI.* The Privacy Rule currently provides individuals with a right to request a restriction on a covered entity's use or

disclosure of PHI for purposes of treatment, payment or health care operations purposes. Until now, covered entities had no corresponding obligation to agree to that request. However, the HITECH Act imposes a new obligation on covered entities to agree to a requested restriction if the disclosure is to a health plan for purposes of payment or health care operations *and* the PHI relates to a health care item or service for which the health care provider has been paid out of pocket in full.⁴⁹

- *Access to PHI.* The HITECH Act requires that in order to fulfill its obligation to provide access to PHI under the Privacy Rule, any covered entity who uses or maintains an EHR must provide an individual with a copy of such information in electronic format or, at the individual's request, transmit the information directly to a person or entity designated by the individual.⁵⁰ The covered entity still may impose a fee for access consistent with the Privacy Rule's requirements, but for providing access under the HITECH Act, the fee must be limited to the covered entity's labor costs in responding to the request.⁵¹

Relationship to Other Laws

The HITECH Act specifically states that HIPAA and the Privacy and Security Rules remain in effect to the extent that they are consistent with the HITECH Act.⁵² HHS is required to amend the Privacy and Security Rules by rulemaking to make them consistent with the HITECH Act.⁵³ In addition, the HITECH Act also states that nothing in the act shall constitute a waiver of privilege otherwise applicable to an individual with respect to PHI.⁵⁴ This provision seems intended to clarify that the new privacy and security provisions of the HITECH Act do not, in and of themselves, effect a waiver of the physician-patient privilege. In recent years, there has been some debate as to whether HIPAA or state privilege law should control in cases in which courts have jurisdiction based on a federal question.⁵⁵

Increased Enforcement and Penalties

The HITECH Act seeks to put more teeth in HIPAA enforcement efforts by increasing civil penalties for HIPAA violations and, in certain cases, requiring formal investigations. These changes appear to respond to charges that the Centers for Medicare and Medicaid Services (CMS), which enforces the Security Rule, and the HHS Office for Civil Rights (OCR), which enforces the Privacy Rule, have been less than rigorous in enforcing HIPAA. In October 2008, these charges took the form of a report from the HHS Office of Inspector General (OIG) that took CMS to task for ineffective and incomplete enforcement of the Security Rule.⁵⁶ In the report, OIG charged that CMS's approach to Security

⁴² ARRA at § 13424(c).

⁴³ ARRA at § 13405(c).

⁴⁴ ARRA at § 13405(c)(1)(A).

⁴⁵ ARRA at § 13405(c)(1)(B).

⁴⁶ ARRA at § 13405(c)(2).

⁴⁷ ARRA at § 13405(c)(4)(A).

⁴⁸ ARRA at § 13405(c)(4)(B).

⁴⁹ ARRA at § 13405(a).

⁵⁰ ARRA at § 13405(e)(1).

⁵¹ ARRA at § 13405(e)(2).

⁵² ARRA at § 13421(b).

⁵³ ARRA at § 13421(b).

⁵⁴ ARRA at § 13421(c).

⁵⁵ See, e.g., *Northwestern Mem'l Hospital v. Ashcroft*, 362 F.3d 923, at 926 (7th Cir. 2004).

⁵⁶ *Nationwide Review of the Centers For Medicare & Medicaid Services Health Insurance Portability And Accountability*

Rule enforcement left “significant vulnerabilities” undetected with respect to electronic medical records at U.S. hospitals.

■ **Enforcement.**

- The HITECH Act requires the secretary of HHS to formally investigate any complaint of a violation of HIPAA if a preliminary investigation indicates a possible violation due to willful neglect, and to impose civil penalties for these violations.⁵⁷
- The HITECH Act also allows state attorneys general to bring civil actions in federal court on behalf of the state’s residents when the attorney general has reason to believe that an interest of one or more residents has been threatened or adversely affected by a person who violates HIPAA.⁵⁸ The attorney general may bring the case to enjoin further action or to obtain damages on behalf of the resident(s).⁵⁹ An attorney general bringing a civil action under HIPAA must give HHS prior written notice of the action, and HHS will have the opportunity to intervene in the action.⁶⁰ If HHS brings an action against a person under HIPAA, then no attorney general may bring an action against the person with respect to the same HIPAA violation while the HHS action is pending.⁶¹

■ **Penalties.**

- Any violation of the HITECH Act is subject to HIPAA civil and criminal penalties.⁶²
- The HITECH Act also creates a tiered approach to civil monetary penalties for violations of HIPAA and the HITECH Act that went into effect immediately upon the law’s enactment. The new tiers are as follows:
 - o If the person did not know (and by exercising reasonable due diligence would not have known) that he or she violated the law, the penalty shall be at least \$100 for each violation not to exceed \$25,000 for all such identical violations during a calendar year, but may be no more than \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.⁶³
 - o If the violation was due to reasonable cause and not to willful neglect, the penalty shall be at least \$1000 for each violation not to exceed \$100,000 for all such identical violations during a calendar year, but may be no more than \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.⁶⁴
 - o If the violation was due to willful neglect AND the violation was corrected, the penalty shall

be at least \$10,000 for each violation not to exceed \$250,000 for all such identical violations during a calendar year, but may be no more than \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.⁶⁵

- o If the violation was due to willful neglect and was not corrected, the penalty shall be at least \$50,000 for each violation not to exceed \$1.5 million for all such violations of an identical requirement or prohibition during a calendar year.⁶⁶
- The HITECH Act requires all civil monetary penalties collected as a result of privacy or security violations to be transferred to OCR to be used for purposes of enforcing the Privacy and Security Rules.⁶⁷
- The HITECH Act also requires the U.S. Comptroller General to issue a report to HHS by Aug. 17, 2010 (18 months after the law’s enactment) that includes recommendations for a methodology under which an individual who is harmed by a HIPAA violation may receive a percentage of the civil monetary penalty collected with respect to that violation.⁶⁸ Based on this U.S. Government Accountability Office (GAO) report, the HITECH Act requires the secretary of HHS to issue regulations by Feb. 17, 2012, setting forth a methodology under which the individual harmed may receive a percentage of the civil monetary penalties collected.⁶⁹
- Significantly, the HITECH Act resolves a point of longstanding confusion in the industry by clarifying that persons who are not covered entities (but who may be employees of covered entities or other individuals) may be found to have violated HIPAA if the PHI is maintained by a covered entity and the person obtained or disclosed such information without authorization.⁷⁰

Privacy Advisers and Educational Initiatives

In addition to increasing enforcement efforts, the HITECH Act also calls for a series of educational initiatives. One set of initiatives will assist covered entities, business associates and others in complying with the relevant privacy and security requirements regarding PHI. Another set of initiatives will educate individuals on the ways in which their PHI may be used or disclosed and their rights with respect to their PHI.

- **Privacy Advisers.** The HITECH Act requires HHS to designate an individual from each regional office to offer guidance and education to covered entities, business associates and individuals regarding federal privacy and security requirements by Aug. 17, 2009.⁷¹
- **Educational Initiatives.** Within one year of enactment, that is, by Feb. 17, 2010, OCR is required to

Act Of 1996 Oversight, Dept. of Health and Human Services Office of Inspector General (October 2008).

⁵⁷ ARRA at § 13410(a)(1)(B).

⁵⁸ ARRA at § 13410(e)(1).

⁵⁹ ARRA at § 13410(e)(1).

⁶⁰ ARRA at § 13410(e)(1).

⁶¹ ARRA at § 13410(e)(1).

⁶² ARRA at § 13410(a)(2).

⁶³ ARRA at § 13410(d)(1)(A).

⁶⁴ ARRA at § 13410(d)(1)(B).

⁶⁵ ARRA at § 13410(d)(1)(C)(i).

⁶⁶ ARRA at § 13410(d)(1)(C)(ii).

⁶⁷ ARRA at § 13410(c)(1).

⁶⁸ ARRA at § 13410(c)(2).

⁶⁹ ARRA at § 13410(c)(3).

⁷⁰ ARRA at § 13409.

⁷¹ ARRA at § 13403(a).

develop and maintain a national education initiative to educate individuals on the potential uses of their PHI and their rights with respect to that information.⁷²

Government Studies and Reports

- *HHS Report on Compliance.* The HITECH Act requires HHS to submit a report to Congress annually regarding complaints received by the secretary alleging violations of health information privacy and security laws.⁷³ The report, which will be posted on the HHS Web site, must include the following information:⁷⁴
 - The number of complaints received;
 - The number and a summary of complaints resolved informally;
 - The number of covered entities that received technical assistance from HHS to achieve compliance and the type of assistance provided;
 - The number of complaints that resulted in civil monetary penalties, including the nature of the complaint and the penalty paid;
 - The number of compliance reviews conducted and the outcome of each review;
 - The number of subpoenas or inquiries issued;
 - HHS’s plan for improving compliance with and enforcement of privacy and security laws over the next year; and
 - The number of audits performed and summary of the findings of each audit.
- *HHS Report on the Application of Privacy and Security Requirements to Non-Covered Entities.* The HITECH Act requires HHS (within one year of enactment) to conduct a study and issue a report to Congress on the applicability of privacy and secu-

rity requirements to non-HIPAA covered entities, including vendors of PHRs, entities that offer products or services through a PHR vendor’s Web site, entities that offer products or services through a covered entity’s Web site who offers PHRs, and any third-party service providers used by any of these entities.⁷⁵ The report must include recommendations for (1) privacy and security requirements, (2) the federal agency best equipped to enforce the requirements and (3) a timeline for implementing the regulations.⁷⁶

- *GAO Report on Treatment Disclosures.* Within one year of the HITECH Act’s enactment, the U.S. Comptroller General is required to issue a report to Congress on the best practices for disclosure of PHI among health care providers for treatment purposes.⁷⁷ The report must address best practices that have been implemented and the extent to which they are successful with respect to the quality of the resulting health care provided and the health care provider’s ability to manage these best practices.⁷⁸ The report also must address the use of electronic informed consent for disclosing PHI for purposes of treatment, payment and health care operations.⁷⁹
- *GAO Report on the Effects of the HITECH Act.* The HITECH Act requires the GAO to issue a report to Congress within five years of its enactment on its impact on health insurance premiums, overall health care costs, adoption of EHRs by providers, and the reduction in medical errors and other quality improvements.⁸⁰

⁷² ARRA at § 13403(b).

⁷³ ARRA at § 13423(a).

⁷⁴ ARRA at § 13423(a)(1)(A) - (G).

⁷⁵ ARRA at § 13424(b).

⁷⁶ ARRA at § 13424(b).

⁷⁷ ARRA at § 13424(d).

⁷⁸ ARRA at § 13424(d).

⁷⁹ ARRA at § 13424(d).

⁸⁰ ARRA at § 13424(e).