

The Stimulus Package: Creating a Nationwide Health Information Technology Infrastructure while Protecting Patient Privacy and Security

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed by President Obama on February 17, 2009. Included in ARRA is the Health Information Technology for Economic and Clinical Health (HITECH) Act that focuses on the development of a nationwide health information technology (HIT) infrastructure that supports electronic health records and health information exchanges.

To accomplish this, the act includes provisions for:

- creating standards, implementation specifications and certification criteria for network interoperability
- implementing the health network and electronic health records (EHRs) through grants, loan funds, incentive programs, and information sharing, and
- encouraging the use of the health network by improving information privacy and security.

Creating and Adopting Standards Necessary to Build a Nationwide HIT Infrastructure

One of the major hurdles to implementing a nationwide HIT infrastructure is the creation of interoperable networks and systems that use commonly accepted standards, implementation specifications and certification criteria. The HITECH Act continues and enhances efforts to develop, adopt and implement these necessary standards.

The Office of the National Coordinator

The act maintains the role of the Office of the National Coordinator for Health Information Technology (ONCHIT, or the national coordinator) by keeping the office in its current form and enhancing its responsibility to lead the development of a nationwide interoperable HIT infrastructure.

The goal of the national coordinator is the use of certified EHRs for every person in the United States by 2014; the development of the EHRs includes the interoperable health information exchanges to share EHRs.

The goal of the national coordinator is the use of certified EHRs for every person in the United States by 2014; the development of the EHRs includes the interoperable health information exchanges to share EHRs. To accomplish this, ONCHIT will update its strategic plan, which was completed on June 3, 2008, and guide the development of standards, implementation specifications and certification criteria.

As part of the standards-development process, ONCHIT will create a framework for exchanging ideas and obtaining participation from the public and individuals who are experts in HIT. It also will use the technical guidance of the National Institute of Standards and Technology (NIST) and other federal agencies. Throughout the process, the national coordinator is required by the HITECH Act to consider privacy, security and strategies to enhance the use of HIT and improve the quality and safety of health care.

The HIT Policy Committee and the HIT Standards Committee

The national coordinator will rely on the HIT Policy Committee and the HIT Standards Committee. The HIT Policy Committee has been created to recommend to ONCHIT a policy framework for the development, adoption, and use of a nationwide HIT infrastructure.

The HIT Standards Committee will oversee the development and pilot testing of standards, implementation specifications, and certification criteria for the HIT infrastructure and make recommendations on them to the national coordinator. The committee also will serve as a forum for the participation of a wide range of stakeholders who will participate and contribute on the development, harmonization and recognition of standards. NIST will assist the committee by testing standards and establishing voluntary testing programs by accredited testing laboratories.

Adoption of Standards

The HITECH Act includes a process for standards adoption. Recommendations for standards will be forwarded by ONCHIT to the Secretary of the Department of Health and Human Services (HHS), who will decide within 90 days whether or not to adopt them. An initial set of standards, implementation specifications, and guidelines shall be adopted by the secretary no later than December 31, 2009.

Pepper Points: Companies interested in including their products and services as part of the nationwide HIT infrastructure should get involved. We have experience with the HIT standards-setting and certification process and can provide counseling and assistance. This includes participation or monitoring the development of standards, implementation specifications, and certification criteria. We can help you by locating the committees or other forums appropriate for your company or by monitoring activities on your behalf.

Promoting HIT through Information Sharing, Medicare and Medicaid Incentive Programs and Grants

The HITECH Act provides funding for investments and programs that promote the adoption of HIT, including EHRs. These include creation of national and regional HIT extension programs, Medicare and Medicaid incentive programs, grants to states, grants for the creation of state loan funds, and grants for educational purposes.

National and Regional HIT Extension Programs

The act calls for the development of HIT extension programs to assist health care providers to adopt, implement and use certified EHRs technology. On the national level, the Health Information Technology Research Center (national center) will assist in the development and recognition of best practices to support and accelerate efforts to adopt, implement and use HIT. This includes technical assistance and analysis and reports on lessons learned from existing private- and public-sector initiatives.

Regionally, Health Information Technology Regional Extension Centers (regional centers) will assist the national center in disseminating information and helping health care providers to implement and use HIT, including EHRs. Through the regional centers, individuals from industry, universities, and state governments will participate in the adoption and use of HIT. The regional centers will act as informational clearinghouses and provide training, and will participate in health information exchanges, where practicable.

Regional centers must be affiliated with a nonprofit institution or organization that applies for and is awarded the financial grant. Funds provided by the federal government for annual operating and maintenance will not exceed 50 percent of the total cost. This cost-sharing requirement may be waived if justified by detrimental national economic conditions.

Medicare and Medicaid Incentives

Although not technically part of the HITECH Act, ARRA contemplates Medicare and Medicaid incentive payments to physicians and hospitals that are “meaningful EHR users” — a physician (as defined under Medicare) who is not hospital-based, or a hospital that (1) demonstrates the use of certified EHR technology in a meaningful manner, such as electronic prescribing; (2) demonstrates that use of EHR technology is connected in a manner that provides for the electronic exchange of health information to improve the quality of care; and (3) submits information on clinic quality measures to HHS using the EHR technology. EHR technology used by the physician or hospital must meet standards adopted by HHS, and the secretary is authorized to make standards for determining “meaningful use” more stringent over time.

An aggressive schedule is provided in ARRA (Title VI of Division B) to use these incentive payments to meet the goal of providing all citizens with EHRs by 2014. For example, certain physicians that quickly demonstrate that they are meaningful EHR users will reap the greatest rewards, of up to approximately \$48,000, through Medicare reimbursements. Incentives also are available through Medicaid programs. A complex incentive payment formula provides hospitals similar incentives under Medicare and Medicaid. Those that fail to meet the goal until 2015 or later will get no reimbursement, and may face penalties from the Centers for Medicare and Medicaid Services (CMS).

Grants to States to Promote HIT

The new law permits the secretary to award a grant to promote HIT to a state or a qualified state-designated entity. These grants may be used to enhance nationwide use and exchange of electronic health information, as well as to provide technical assistance toward achieving a nationwide infrastructure.

Initially, states may not be required to contribute additional funding beyond the federal dollars provided under the grant. However, beginning in fiscal year 2011, a non-federal contribution of 10 percent; this match of funds increases to 14 percent in fiscal year 2012 and to 33 percent in fiscal year 2013.

Competitive Grants to Develop Loan Programs to Promote Adoption of Certified EHR Technology

Competitive grants to a state or a Native American tribe are provided under the HITECH Act to establish certified EHR technology. The grants will be deposited in a loan fund, from which grants will be provided directly to health care providers.

Loans may be used by the providers to (i) facilitate the purchase of certified EHR technology; (ii) enhance the use of the technology, which may include the costs of upgrading technology so that it meets criteria to be certified EHR technology; (iii) train personnel in using such technology; or (iv) improve the secure electronic exchange of health information.

Certain physicians that quickly demonstrate that they are meaningful EHR users will reap the greatest rewards, of up to approximately \$48,000, through Medicare reimbursements.

Grants for Educational Purposes

Higher education institutions also can get grant funds to carry out demonstration projects to develop academic curricula integrating certified EHR technology into health professionals' clinical education. Grants provided under this program are to be used for community-based clinical education involving the collaboration of two or more disciplines. The funds may not be used to purchase hardware, software or services. Awards are competitive and will be granted pursuant to peer review.

In another program, financial assistance may be provided to medical health informatics education programs to ensure rapid, effective development and use of health information technologies. This includes certification, undergraduate and master's degree programs for both health care and information technology students.

The assistance will be provided by the secretary in consultation with the National Science Foundation and may include developing and revising curricula, recruiting and retaining students, acquiring equipment, and establishing or enhancing bridge programs between community colleges and universities. In providing assistance, the secretary will give preference to existing education and training programs and programs designed to be completed in fewer than six months.

For both of these grants, the government will provide up to 50 percent of the costs for any activity for which assistance is provided. This cost-sharing requirement may be waived if justified by detrimental national economic conditions.

Pepper Points: You have plenty of opportunities in this bill to indirectly promote your product and service, through incentives, grants and extension centers. We can assist you

by monitoring how the grants are rolled out and notify you as opportunities arise. We can steer you through the grant application process. We can analyze the Medicare and Medicaid incentives available to eligible health care providers to help you pitch your HIT products to them.

Encouraging the Nationwide HIT Infrastructure by Improving Privacy and Security

The HITECH Act recognizes that the successful adoption of HIT relies on privacy and security. The act includes provisions intended to enhance and strengthen privacy and security of health information as it is received, created, processed, stored and transmitted over the nationwide HIT infrastructure. These key provisions include:

- clarification and expansion of the definition of a “business associate”
- increased business associate legal obligations
- notification for breaches involving protected health information (PHI)
- special provisions for vendors of personal health records and other non-HIPAA covered entities, and
- enhancement of enforcement, funding for enforcement and increased penalties.

Recasting the Definition of a ‘Business Associate,’ and Their Increased Legal Obligations

The HITECH Act includes as business associates entities that provide data transmission services to a covered entity (or its business associate) if the service routinely involves access to PHI. This includes, for example, a health information exchange organization, a regional health information organization, an e-prescribing gateway, or any vendor that contracts with the covered entity to allow the entity to offer a personal health record (PHR) to patients.

Enhancing the Business Associate’s Legal Obligations

The HITECH Act amends the HIPAA security rule by providing that business associates must comply with the same administrative, technical and physical safeguards that a covered entity must comply with under the security rule. Training of employees is required as part of the administrative safeguards. A business associate also must prepare and implement policies and procedures, and other documents required by the security rule. These changes will enhance the business associate’s information security practices, and

better enable a covered entity to monitor a business associate’s information security program.

The legislation provides that each security and privacy requirement in the act that applies to a covered entity also applies to a business associate.

The act provides that business associates that violate HIPAA’s security and privacy provisions are subject to the same civil and criminal penalties as a covered entity.

Notifications for Breaches Involving Protected Health Information

The HITECH Act provides notice of breach provisions. It applies to business associates and covered entities that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI. A “breach of security” is an acquisition, access, use or disclosure of unsecured (i.e., unencrypted) PHI.

The act requires any encryption technology used to be developed or endorsed by a standards developing organization accredited by the American National Standards Institute, or otherwise through the use of technology or methodology specified by the secretary.

- **Breaches Experienced by a Covered Entity**

Following the discovery of a breach, a covered entity shall notify each individual whose unsecured PHI has been, (or is reasonably believed to have been) accessed, acquired or disclosed as a result of the breach.

Notice must include a brief description of what happened and when, an accounting of the PHI that was compromised, what individuals must do to protect themselves, and a brief description of how the covered entity responded to the breach. Also required are identification of the covered entities, their contact information, and ways people can get further information about the breach from the covered entity.

A covered entity or a business associate (including any employee, officer, or other agent of the entity or associate other than the individual committing the breach) should consider a breach “discovered” on the day they first know of it, or reasonably should have known it had occurred. Unless delayed for law enforcement purposes, notifications must be prompt, never later than 60 days after the breach is discovered.

Notice may be written and sent by mail or e-mail. If mailing or e-mail addresses are unavailable or insufficient, substitute notice may be provided by placing a conspicuous posting on the home page of the covered entity's Web site or via major print or broadcast media. Substitute notice must include a toll-free number that people can call to learn whether their unsecured PHI is included in the breach. The covered entity may notify individuals by telephone or other means as appropriate, if the possible imminent misuse of unsecured PHI make notification urgent. Notice also may be provided to the media if the breach of PHI involves more than 500 individuals.

Breaches involving more than 500 people must be reported immediately to the secretary. Breaches involving fewer than 500 people must be logged and then annually submitted to the secretary. The secretary will post on its Web site a list of covered entities involved in breaches of more than 500 people, and also shall provide annual reports of breaches to specified House committees.

- **Breaches Experienced by a Business Associate**

A business associate must notify the covered entity following the discovery of a breach. The notice must identify each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during the breach.

Notice of Breach Involving Vendors of Personal Health Records and Other Non-HIPAA Covered Entities

The HITECH Act differentiates between an EHR and a personal health record (PHR). An EHR is an electronic record of health-related information about an individual, created, gathered, managed and consulted by authorized health care clinicians and staff. A PHR can be drawn from multiple sources and is managed, shared, and controlled by or primarily for the individual. "PHR identifiable health information" is an electronic record of individually identifiable health information that:

- is provided by or on behalf of the individual, and
- identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Additional provisions for notice of breaches apply to "PHR-related entities," which are: (i) vendors of PHRs; (ii) entities that offer products or services through the Web site of a vendor of PHRs; (iii) entities that are not covered entities and that offer products or services through the Web site of covered entities that offer individuals' personal health records; and (iv) entities that are not covered entities that access information in PHRs or send information to a PHR.

A "breach of security" means a person's unsecured PHR identifiable health information was acquired without that person's authorization. When a PHR-related entity discovers a breach of the security of an unsecured PHR, the entity shall notify each citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of the breach.

The PHR-related entity also must notify the Federal Trade Commission, which in turn will notify the secretary of the breach. A violation of the breach requirements will be treated as an unfair and deceptive act or practice in violation of the regulations under the Federal Trade Commission Act, and will be enforced as such.

The requirements for timing, method and content of notifications are the same as those applying to covered entities. Similarly, PHR identifiable health information is unsecured when it is not encrypted.

The notice provisions also apply to a third-party service provider that handles PHR identifiable health information on behalf of a PHR-related entity. The service provider must notify the PHR-related entity following discovery of the breach and identify each individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, accessed, acquired or disclosed during the breach.

Enhanced Enforcement and Penalties

The HITECH Act will beef up enforcement of HIPAA by adding new penalties, enforcement mechanisms and penalties. The following is an overview of the key changes.

Clarification of the Crime of Wrongful Disclosure of Individually Identifiable Information

The current statute defines the wrongful disclosure of individually identifiable information as follows:

(a) Offense

A person who knowingly and in violation of this part – when a person knowingly and in violation of HIPAA –

1. uses or causes to be used a unique health identifier
2. obtains individually identifiable health information relating to an individual, or
3. discloses individually identifiable health information to another person

shall be punished as provided in subsection (b) of this section. (42 U.S.C. §1320d-6.)

The HITECH Act amends this definition, by clarifying that for a crime to be committed a person must obtain or disclose individually identifiable information without authorization, by adding at the end of the first sentence the following:

For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulations described in section 1180(b)(3)) and the individual obtained or disclosed such information without authorization. (*Id.*, §13409)

Penalties for criminal violations have not changed. The base penalty is a \$50,000 fine, imprisonment for not more than one year, or both. For offenses committed under false pretenses, the fine is not more than \$100,000, imprisonment for not more than five years, or both. And if the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, the fine is not more than \$250,000, imprisonment for not more than 10 years, or both.

The HITECH Act provides that any HIPAA violation by a covered entity may be subject to enforcement and penalties under HIPAA's criminal and civil provisions. However, a

The legislation provides that each security and privacy requirement in the act that applies to a covered entity also applies to a business associate.

civil penalty cannot be imposed if a criminal penalty has been imposed for the same violation.

New Civil Violation of “Willful Neglect”

The HITECH Act includes civil investigation and action for noncompliance due to willful neglect. A formal investigation will begin whenever a preliminary investigation reveals that a possible violation is due to willful neglect. A final finding of noncompliance due to willful neglect will be subject to HIPAA civil penalties.

Civil Monetary Penalty Tiers and Increase of Penalty Amounts

The HITECH Act has established the following tiers for civil penalties:

1. \$100 per violation, except that the total amount imposed on a person for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000.
2. \$1,000 per violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed \$100,000.
3. \$10,000 per violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed \$250,000.
4. \$50,000 per violation, except that the total amount imposed on a person for all such violations of an identical requirement or prohibition during a calendar year may not exceed \$1.5 million.

The penalties, depending on degree of knowledge and culpability concerning the violations, will range as follows:

- **Without Knowledge.** When established that a person

did not know (and by exercising reasonable diligence would not have known), the penalty for each violation will be at least the amount in paragraph 1 but not exceed the amount in paragraph 4.

- **Reasonable Cause.** When established that the violation was due to a reasonable cause and not to willful neglect, a penalty for each such violation will be at least the amount in paragraph 2 but not exceed the amount in paragraph 4.
- **Willful Neglect.** When established that the violation was due to willful neglect, a penalty for each such violation will be at least the amount in paragraph 3, but not exceed the amount in paragraph 4 when the violation is corrected, or at least the amount in paragraph 4 if the violation is not corrected.

Funding Mechanism for Enforcement and Audits

Any civil monetary penalty or settlement collected with respect to a criminal or civil action brought under HIPAA's security and privacy provisions shall be transferred to the Office for Civil Rights of the HHS. This money will fund enforcing HIPAA's privacy and security provisions.

The HITECH Act calls for a study by the U.S. General Accountability Office to determine:

- the feasibility of distributing to victims of a violation a percentage of any collected civil monetary penalty or settlement, and
- the methodology to accomplish the distribution.

Enforcement by State Attorneys General

In any case in which the attorney general of the state has reason to believe that an interest of one or more of the state's residents has been or is threatened or adversely affected by anyone who violates the provisions of HIPAA, the attorney general, as *parens patriae*, may bring a civil action on behalf of those residents in a U.S. district court. The attorney general bringing an action may enjoin further violations by the defendant or obtain damages on behalf of the residents.

Damages will be statutorily imposed. The amount is calculated by multiplying the number of violations by up to \$100. However, the total amount of damages imposed on the person for violations of all identical requirements or prohibition during a calendar year shall not exceed

\$25,000. The court may also award the attorney general reasonable costs for bringing the action and attorney's fees.

The state will provide the secretary with written notice and a copy of the complaint for any action brought by the attorney general. The secretary will have the right to intervene in the action. Upon intervening, the secretary will be heard on all matters pertaining to the case and be permitted to file petitions for appeal. If the secretary has instituted an action against a person with respect to a specific violation, the state attorney general may not bring an action with respect to the same violation during pendency of the federal action.

The amendments made by this subsection shall apply to violations occurring after the HITECH Act is enacted.

Additional Provisions

A number of the HITECH Act's new provisions pertain to privacy and security. In summary, they are:

- **Restrictions on certain disclosures.** Individuals will have the right to prohibit the disclosure of PHI to a health plan for items or services that the individual paid for in full out-of-pocket.
- **Minimum Necessary Rule.** New regulations will be released clarifying the "minimum necessary" PHI that may be disclosed in limited data sets and for other purposes.
- **Restrictions on sales of EHRs or PHI.** Covered entities and business associates may not sell PHI and EHRs, except in limited circumstances, unless the individual authorizes the sale.
- **Accounting of certain PHI disclosures required if covered entity uses an EHR.** Covered entities must provide accounting for disclosure of PHI to carry a treatment, payment, and health care operations when the PHI is in an EHR.
- **Access to certain information in electronic format.** An individual has a right to obtain from the covered entity a copy of his or her information in an electronic format.
- **Conditions on certain communications as part of health care operations.** Limits the health care operations exception for communications when the covered entity is paid for the communication except in limited circumstances.

Pepper Points: The new privacy and security requirements the HITECH Act imposes affect a large number of covered entities, business associates and non-HIPAA covered entities. We can help in a number of ways. We can assist you in understanding these changes and analyze how they affect your organization. We have the qualifications and experience to conduct mini-assessments of the legal compliance of your information security and privacy practices and help you integrate these changes into your current compliance program. We will help non-HIPAA covered entities build a program that complies with HIPAA. We offer counseling to banks and other business associates that will be involved in the nationwide HIT infrastructure on whether and how to amend their business associate agreements to comply with the new requirements and integrate the HIPAA security rules into current security and privacy programs. We can analyze for data warehousing organizations how the prohibitions on the sale and marketing of PHI and EHRs affect operations. We can provide training, policies and procedures and tips on implementation of all the requirements.

Authors:

*M. Peter Adler
202.220.1278
adlerp@pepperlaw.com*

*Sharon R. Klein
949.567.3506
215.981.4172
kleins@pepperlaw.com*

This is one of a series of articles published by members of Pepper Hamilton LLP discussing issues arising out of the American Recovery and Reinvestment Act of 2009. For our other publications, please refer to our firm's Web site at www.pepperlaw.com.

Pepper Hamilton LLP Attorneys at Law

The material in this publication is based on laws, court decisions, administrative rulings and congressional materials, and should not be construed as legal advice or legal opinions on specific facts. The information in this publication is not intended to create, and the transmission and receipt of it does not constitute, a lawyer-client relationship.

Please send address corrections to phinfo@pepperlaw.com.

www.pepperlaw.com

Berwyn | Boston | Detroit | Harrisburg | New York | Orange County
Philadelphia | Pittsburgh | Princeton | Washington, D.C. | Wilmington

© 2009 Pepper Hamilton LLP. All Rights Reserved.

This publication may contain attorney advertising.