



Health Law Pulse

ATTORNEY ADVERTISING

MARCH 2009

Health Care Implications of Federal Stimulus Plan

IN THIS ISSUE:

- Health Information Technology
- Medicare and Medicaid Incentives for Use of EHR Technology
- Privacy and Security

On February 17, 2009 (the "Enactment Date"), the American Recovery and Reinvestment Act of 2009 (the "Act") was signed into law. The Act provides, among other things, funding for the development and implementation of health information technology ("HIT"), Medicare and Medicaid financial incentives for health care providers that implement and use electronic health records ("EHR"), and additional privacy and security rules for entities subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") ("covered entities"), business associates, vendors of personal health records and other similar entities. The health care provisions in the Act are generally effective 12 months after the Enactment Date, unless otherwise noted in this article. A summary of the key health care provisions of the Act is provided below.

Health Information Technology

Infrastructure

In the area of HIT, the Act establishes the Office of the National Coordinator for Health Information Technology (the "National Coordinator"). The National Coordinator is responsible for furthering the development of a nationwide HIT infrastructure that allows for the electronic use and exchange of information according to certain defined principles, including health care quality and security of information. The Act provides \$2 billion to the National Coordinator to carry out its purposes. The National Coordinator is authorized to create several new programs related to the electronic exchange of health information, including grants for:

- universities and other institutions of higher education to establish multidisciplinary Centers for Health Care Information Enterprise Integration ("Centers") which will be responsible for researching current challenges to health care delivery and the role of health information technologies in meeting those challenges.
- states, or qualified state-designated entities, to facilitate and expand the electronic transmission and use of health information among organizations in accordance with nationally recognized standards. To be a qualified state-designated entity, the entity must show that it (i) has been designated by a state to receive the grant, (ii) is a not-for-profit entity with broad stakeholder representation on its board of directors, (iii) has a principal goal of improving health care quality and efficiency through the use of electronic health information, (iv) has adopted nondiscrimination and conflict of interest policies, and (v) conforms with other requirements provided by the Secretary of the Department of Health and Human Services ("HHS") (the "Secretary").
- states and Indian tribes to establish EHR technology loan funds for providers to acquire and implement EHR technology.
- demonstration projects to develop academic programs that integrate EHR technology into the clinical education of health professionals.

The National Coordinator is also tasked with the development of standards, implementation specifications and certification criteria for the electronic exchange and use of health information. The Secretary must adopt an initial set of standards, implementation specifications and certification criteria no later than December 31, 2009. The National Coordinator is charged with designating entities to be responsible for harmonizing and updating such standards to achieve a uniform and consistent implementation. The Act establishes a HIT Standards Committee and a HIT Policy

Committee to assist in this effort.

Comparative Effectiveness Research

The Act provides \$1.1 billion for comparative effectiveness research (i.e. research which compares different health care treatments and strategies to determine their effectiveness). Of the total amount, \$300 million is allocated to the Agency for Healthcare Research and Quality, \$400 million is allocated to the National Institutes of Health, and \$400 million is allocated to HHS. Additionally, the Act establishes the Federal Coordinating Council for Comparative Effectiveness Research with the goal of reducing duplicative research efforts and encouraging the coordinated use of resources.

Federally Qualified Health Centers

The Act provides \$1.5 billion for grants through HHS's Health Resources and Services Administration for construction, renovations and equipment and for the acquisition of HIT systems by federally qualified health centers ("FQHCs") receiving grants under Section 330 of the Public Health Service Act. An additional \$500 million in grants is authorized for such FQHCs without limitations on usage.

Prevention and Wellness Fund

The Act creates a \$1 billion "Prevention and Wellness Fund" under HHS. Of this amount, \$300 million is transferred to the Centers for Disease Control and Prevention for funding immunization programs under the Public Health Service Act, \$650 million is allocated for evidence-based clinical and community-based prevention and wellness strategies to address chronic disease rates, and \$50 million is allocated to the states to offset the cost in implementing reduction strategies for health care-associated infections.

Medicare and Medicaid Incentives for Use of EHR Technology

The Act sets aside \$17.2 billion in incentive payments under Medicare and Medicaid to eligible professionals and eligible hospitals for "meaningful use" of certified EHR technology. Under the Act, meaningful use by a professional or hospital means (i) using certified EHR technology in a meaningful manner, including the professional's use of electronic prescribing; (ii) demonstrating that such certified EHR technology provides for the electronic exchange of health information to improve the quality of health care, such as promoting care coordination; and (iii) submitting information on clinical quality measures through the use of EHR. For purposes of the Act, an eligible professional under Medicare is a doctor of medicine or osteopathy, a doctor of dental surgery or dental medicine, a doctor of podiatric medicine, a doctor of optometry, or a chiropractor. Under Medicaid, an eligible professional includes a physician, dentist, certified nurse-wife, nurse practitioner, or a physician assistant practicing in a physician assistant-run rural health clinic or an FQHC (eligible professionals under Medicare or Medicaid are referred to generally in this article as "Eligible Professionals").

Medicare Incentives to Eligible Professionals

In addition to the Medicare payments that an Eligible Professional receives for patient services, an Eligible Professional can receive Medicare incentive payments in an amount equal to 75% of such professional's allowed charges based on claims submitted by such professional. The maximum amount of Medicare incentive payments that an Eligible Professional can receive is provided below. The incentives will begin in fiscal year 2011 and will continue for five years. No incentive payments will be given if the implementation and use of EHR first occurs after fiscal year 2014. If an Eligible Professional has not demonstrated meaningful use of EHR technology by fiscal year 2015, Medicare will penalize such professional by reducing the Medicare reimbursement that he or she receives. Hospital-based professionals generally will not qualify for Medicare incentives. The incentives for Eligible Professionals providing services in a health professional shortage area ("HPSA") will be increased by 10%.

An Eligible Professional demonstrating meaningful use of EHR will be eligible to receive up to the following amounts:

Implementation Year	Amount of Payment
Initial year of EHR use	\$18,000, if first use occurs in 2011 or 2012; \$15,000, if first use occurs in 2013; \$12,000, if first use occurs in 2014.
Second year of EHR use	\$12,000
Third year of EHR use	\$ 8,000
Fourth year of EHR use	\$ 4,000
Fifth year of EHR use	\$ 2,000

No Medicare incentive payments will be given to Eligible Professionals after 2016. Therefore, if an Eligible Professional first meets the meaningful use requirements in fiscal year 2014, he or she will only be eligible to receive incentive payments for two additional years. Eligible Professionals who have already implemented EHR, or implement EHR by 2011, may be eligible to receive the total maximum incentive payments of \$44,000 over the five-year period of 2011 to 2016.

Medicaid Incentives to Eligible Professionals

Eligible Professionals may receive 85% of their average annual EHR costs, which includes costs for support,

maintenance and training (as more specifically described in the Act), less amounts received for such EHR costs from other sources, subject to a limit of \$25,000 for first-year costs and \$10,000 annually thereafter. Eligible Professionals are eligible for Medicaid incentives if 30% of their services are provided to Medicaid patients (20% for pediatricians) and they waive their rights to Medicare incentives. Hospital-based professionals are not eligible for Medicaid incentives. The Medicaid incentive payments will begin in 2011. Eligible Professionals can receive these incentives for a period of five years, the first year being when the Eligible Professional demonstrates an effort to adopt, implement, or upgrade EHR technology. To qualify in subsequent years, the Eligible Professional must demonstrate meaningful use of EHR (as provided above under *Medicare Incentives*). Medicaid incentive payments cannot begin after 2016 and no payments will be made after 2021.

Medicare Incentives to Hospitals

Eligible Hospitals (as defined below) will receive Medicare incentive payments for meaningful use of EHR beginning in 2011. As with Eligible Professionals, if a hospital's EHR implementation and use does not occur by 2015, the Act phases in Medicare payment penalties by reducing the hospital's Medicare reimbursement. Eligible Hospitals do not include rehabilitation hospitals, hospitals where patients are predominantly under 18 years old, hospitals with average inpatient stays of greater than 25 days, or hospitals involved extensively in the treatment or research of cancer. Medicare incentive payments for an Eligible Hospital are calculated according to a formula set forth in the Act which takes into account the Eligible Hospital's Medicare bed days and discharges. The incentive decreases each year after implementation over a 5-year period. Critical access hospitals will obtain Medicare incentive payments by submitting in their annual cost report the costs associated with EHR technology for the given year.

Medicaid Incentives to Hospitals

Children's hospitals and acute care hospitals that are not children's hospitals, but have at least a 10% Medicaid patient volume, will be eligible to receive Medicaid incentives similar to the Medicare incentives above. Medicaid incentive payments are calculated similarly to Medicare incentive payments, but the formula substitutes Medicaid bed days for Medicare bed days. The Medicaid incentive payments will begin in 2011 and such hospitals can receive these incentives for a period of 6 years. The first year of payment cannot begin after 2016 and no payments will be made after 2021.

Privacy and Security

The Act enhances privacy and security protections for protected health information ("PHI") by making a number of significant changes to the obligations of covered entities and business associates.

Business Associates

Business associates are persons and entities who provide services to covered entities requiring the use or disclosure of individually identifiable health information. Prior to the Act, business associates were not directly subject to HIPAA's privacy and security rules, but were required to contractually protect the privacy of a covered entity's PHI in accordance with a "business associate agreement" with the covered entity. Under the Act, business associates of covered entities will be subject to many new requirements.

The Act's new security and privacy requirements applicable to covered entities also apply to business associates and must be incorporated into the business associate agreement between the business associate and the covered entity. In addition, business associates of covered entities are also required to implement administrative, physical, and technical safeguards to protect the electronic PHI that it creates, receives, transmits, and maintains and policies and procedures for documentation of compliance with the security standards in the same manner that a covered entity has to implement such measures. The implementation of such safeguards and policies and procedures must be incorporated into the business associate agreement between the business associate and the covered entity.

Currently under HIPAA, a covered entity is required to take reasonable steps to cure a breach or violation of a business associate agreement by the covered entity's business associate and to terminate the agreement with the business associate or notify the Secretary if the business associate does not cure the breach. Under the Act, the business associate has these same obligations if a covered entity breaches the business associate agreement. Specifically, if a business associate has knowledge of a covered entity's breach of a business associate agreement, the business associate must take reasonable steps to cure the breach or end the violation and if such steps are unsuccessful, the business associate must either terminate the agreement with the covered entity or notify the Secretary if termination of the agreement is not feasible.

Furthermore, under the Act, business associates are now required to notify covered entities upon discovery of a breach of PHI that is not secured by an appropriate technology standard that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals (or a standard that is otherwise defined in guidance to be issued by the Secretary)("Unsecured PHI"). The notice must be made "without unreasonable delay" and in no case later than 60 days after the discovery of the breach, and must include the identification of each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed or disclosed during the breach. This requirement is effective 30 days after the date that the Secretary promulgates interim final regulations that address such requirement.

The Act subjects business associates to the same civil and criminal penalties that apply to covered entities.

Security Breach Notification

Under the Act, any covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise

holds, uses, or discloses Unsecured PHI is now required to notify each individual whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired, or disclosed ("Affected Individual") as a result of a breach of PHI. The covered entity must provide written notification to the Affected Individual (or by electronic mail if the Affected Individual has specified such preference) at the last known address of such individual or next of kin without unreasonable delay and in no case later than 60 days after the discovery of such breach. In the event that the covered entity does not have current contact information for the Affected Individual, the covered entity must provide notification through a substitute form. Regardless of the method of notice, the notification must include (i) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (ii) a description of the types of Unsecured PHI that were involved in the breach (i.e. full name, social security number, date of birth, home address, account number, or disability code); (iii) the steps the Affected Individuals should take to protect themselves from potential harm resulting from the breach; (iv) a brief description of what the involved covered entity is doing to investigate the breach, mitigate losses, and protect against any further breaches; and (v) contact procedures that Affected Individuals can use to ask questions or learn additional information, including a toll-free telephone number, e-mail address, Web site, or postal address.

If there is a breach that affects 10 or more Affected Individuals, the covered entity must provide a conspicuous posting for a period determined by the Secretary on the home page of its Web site or notice in major print or broadcast media. Such conspicuous posting must include a toll-free telephone number where individuals can learn whether their Unsecured PHI was included in the breach. The covered entity is also required to maintain a log of any breaches that affect less than 500 Affected Individuals and annually submit such log to the Secretary. If there is a breach that affects more than 500 Affected Individuals, the covered entity must provide notice to prominent media outlets serving the state in which the breach occurred and notify the Secretary immediately of such breach. If a law enforcement official determines that a notification (as provided above) would impede a criminal investigation or cause damage to national security, such notification, notice, or posting must be delayed.

The Secretary will promulgate interim final regulations no later than 180 days after the Enactment Date. These security breach notification requirements are effective 30 days after the date that the Secretary promulgates the interim final regulations.

It is important to note that many states, including Connecticut and Massachusetts, already have statutes that require notice of security breaches and such statutes may contain additional or different requirements.

Breach Notification Requirements for PHR Vendors and PHR-related Entities

The Act places similar notification requirements on personal health record ("PHR") vendors and other PHR-related entities. PHR-related entities include entities that offer products or services through a PHR vendor's Web site, noncovered entities that offer products or services through a covered entity's Web site that offer individuals PHR, and noncovered entities that access information in a PHR or send information to a PHR ("PHR-related Entities").

Under such requirements, PHR vendors and PHR-related Entities must notify Affected Individuals and the Federal Trade Commission ("FTC") whenever there is a breach of security of Unsecured PHI located in a PHR ("PHR Information"). A third-party service provider that provides services to a PHR vendor or a PHR-related Entity and accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR Information is required to notify each PHR vendor or PHR-related Entity in the event of a breach of security upon discovery of such breach. This notice must include the identification of each individual whose unsecured PHR Information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. Failure on the part of a PHR vendor, PHR-related Entity, or third-party service provider to provide the required notice of a breach will be considered an unfair and deceptive act or practice in violation of the FTC Act.

The Act directs the FTC to publish interim final regulations to carry out these provisions no later than 180 days after the Enactment Date. These provisions will apply to breaches of security that are discovered 30 days or more after the publication of such interim final regulations.

Education on Health Information Privacy

Within 6 months after the Enactment Date, the Secretary will designate an individual in each regional office of HHS to offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirements for PHI. Similarly, within 12 months of the Enactment Date, the Office of Civil Rights within HHS will develop and maintain a multifaceted national education initiative to enhance public transparency regarding the uses of PHI, including programs to educate individuals about the potential uses of their PHI, the effects of such uses, and the rights of individuals with respect to such uses.

Requested Restrictions on Certain Disclosures of PHI

HIPAA's privacy rules provide that individuals may request a restriction of the uses and disclosures of their PHI, but that the covered entity is not required to agree to such restriction. The Act provides that a covered entity cannot use or disclose PHI if an individual requests a restriction from use or disclosure except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment) if the PHI pertains solely to a health care item or service for which the health care provider involved was paid out-of-pocket in full.

Limited Data Sets and Minimum Necessary

The Act specifies that to be in compliance with HIPAA's minimum necessary standard with respect to the use,

disclosure, or request of PHI, covered entities must limit such PHI, to the extent practicable, to a limited data set, or if needed by the covered entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. The minimum necessary standard does not apply in certain circumstances, including disclosures to and requests by a health care provider for treatment purposes. The Secretary will be issuing guidance on what constitutes "minimum necessary" within 18 months of the Enactment Date.

Accounting of Disclosures

An individual currently has the right to receive an accounting of disclosures of his or her PHI made by a covered entity during the 6 years prior to the date on which the accounting is requested. Covered entities are not currently required to provide an accounting of disclosures that are made to carry out treatment, payment and health care operations. Under the Act, covered entities that use or maintain EHR with respect to PHI are now required to provide an accounting of disclosures of electronic PHI that were made to carry out treatment, payment, and health care operations during the 3 years prior to the date on which the accounting is requested ("New Accounting Rules"). In response to an individual's request, a covered entity can provide either an accounting of disclosures of PHI (i) that are made by such covered entity and by a business associate acting on behalf of the covered entity, or (ii) that are made by such covered entity and a list of all business associates acting on behalf of the covered entity, including contact information for such business associates. Any business associate included in such list will be required to provide an accounting of disclosures made by such business associate to the individual requesting such information.

A covered entity that began using EHR before January 1, 2009 is not subject to the New Accounting Rules until January 1, 2014. A covered entity that began using EHR after January 1, 2009 is not subject to the New Accounting Rules until the later of January 1, 2011 or the date that it acquires an EHR. The Secretary will issue regulations addressing the specific information that a covered entity will need to collect about each disclosure within 6 months of adopting general standards on accounting for disclosures.

Sale of EHR or PHI

Under the Act, a covered entity or business associate cannot directly or indirectly receive payment in exchange for an individual's PHI unless it obtains from such individual a valid authorization that specifies that the covered entity or business associate is being paid for the disclosure of such PHI ("Sale of PHI Rules"). The Sale of PHI Rules do not apply where the purpose of the exchange is for (i) public health activities; (ii) research, as long as the price charged reflects the costs of preparation and transmittal of the data for such purpose; (iii) the treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent PHI from inappropriate access, use, or disclosure; (iv) health care operations; (v) remuneration that is provided to a business associate for activities involving the exchange of PHI that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement; (vi) providing an individual a copy of his or her PHI; or (vii) other purposes as identified in regulations by the Secretary.

The Sale of PHI Rules are effective 6 months after the Secretary promulgates regulations that address the Sale of PHI Rules. The Secretary will promulgate such regulations within 18 months of the Enactment Date.

Access to Electronic PHI

The Act clarifies that an individual has a right to obtain a copy of his or her PHI in electronic format from a covered entity that maintains EHR. Additionally, an individual may request that the electronic copy of his or her PHI be transmitted directly to an entity or person designated by such individual. The covered entity may impose a fee for providing an individual an electronic copy of his or her PHI that is no greater than such covered entity's labor costs in responding to the request for the electronic copy.

Marketing Communications

HIPAA defines "marketing" as any communication that encourages recipients of such communication to purchase or use the product or service marketed. While a covered entity must obtain an individual's authorization prior to using his or her PHI for marketing purposes, a covered entity does not have to obtain an individual's authorization when the communication is made (i) to describe a health-related product or service that is provided by or included in the covered entity's plan of benefits, (ii) for the treatment of the individual, or (iii) for case management or care coordination for the individual ("Non-marketing Communications").

Under the Act, if the covered entity or business associate has received direct or indirect payment (not including payment for treatment) in exchange for making a Non-marketing Communication, then such communication will only remain a Non-marketing Communication if it (i) describes a drug or biologic product that is currently being prescribed for the individual receiving the communication and any payment received by the covered entity in exchange for making such communication is reasonable, (ii) is made by the covered entity and such covered entity has obtained a valid authorization from the individual receiving the communication, and (iii) is made by a business associate on behalf of the covered entity and the communication is consistent with a written contract between such business associate and covered entity. The Secretary will define reasonable payment in a future regulation.

Fundraising Communications

The Act directs the Secretary to issue a rule that allows an individual to elect not to receive written fundraising communications, even if those communications are considered health care operations. Such an election on the part of an individual will be considered a revocation of authorization to use or disclose such individual's PHI.

Enforcement

Currently, an individual or organization that fails to comply with the HIPAA regulations due to willful neglect is subject to monetary fines unless such failure is corrected within a 30-day period beginning after the individual knew or should have known that a violation occurred. An individual or organization that knowingly fails to comply with the HIPAA regulations is subject to both monetary fines and imprisonment.

The Act strengthens HIPAA's enforcement provisions by creating a tiered scheme for civil monetary penalties for HIPAA violations. An individual or organization that unknowingly violates HIPAA is subject to at least a \$100 penalty per violation. An individual or organization that violates HIPAA as a result of reasonable cause (and not willful neglect) is subject to at least a \$1,000 penalty per violation. As for an individual or organization that violates HIPAA due to willful neglect, the Secretary will conduct a formal investigation of any HIPAA violation that is the result of willful neglect. If, after such investigation, the Secretary concludes that a violation was in fact the result of willful neglect but such violation has been corrected, a fine of not less than \$10,000 (but not more than \$50,000) will be imposed for each violation, not to exceed \$1,500,000 per year. If such a violation has not been corrected, a fine of \$50,000 will be imposed for each violation, not to exceed \$1,500,000 per year. In determining the amount of the penalty, the Secretary will consider the nature and extent of the violation and harm resulting from such violation.

The Act also provides state attorneys general with authority to enforce the HIPAA regulations by filing a civil action against a person or organization that has violated HIPAA. A state claim may not be filed if a federal claim is pending. Furthermore, state attorneys general have significant limits on their authority to collect monetary damages. The Act states that damages sought by a state attorney general should be calculated by multiplying the number of violations by an amount up to \$100. A court may consider several factors in determining the amount of a penalty. Attorneys general may also recover attorneys' fees and other costs related to such actions in the event that a successful claim is made by a state.

These enforcement provisions are subject to a 6-year statute of limitations period and apply to violations occurring after the Enactment Date.

HHS Audits

Under the Act, HHS will periodically audit covered entities and business associates to ensure their compliance with HIPAA's privacy and security rules.

The Act significantly impacts the health care industry by providing many benefits and imposing new restrictions on covered entities, business associates, vendors of PHR and PHR-related Entities. Specifically, the Act provides funding to health care providers for the development and implementation of HIT, including substantial incentives from Medicare and Medicaid, and penalizes health care providers who do not implement such HIT prior to the year 2015. While promoting the implementation of HIT, the Act enhances the privacy and security requirements under HIPAA, broadens the reach of such privacy and security requirements, and heightens the Secretary's enforcement of such privacy and security requirements.

If you have any questions regarding how the Act affects your operations, please feel free to contact any member of Robinson & Cole's Health Law Group.

Robinson & Cole's Health Law Group includes:

<u><i>Lisa M. Boyle</i></u>	<u><i>Theodore J. Tucci</i></u>
<u><i>Michael J. Kolosky</i></u>	<u><i>Karen P. Conway</i></u>
<u><i>B. Moses Vargas</i></u>	<u><i>Brian D. Nichols</i></u>
<u><i>Susan E. Roberts</i></u>	<u><i>Kimberly E. Troland</i></u>

For more information, please contact Lisa Boyle at lboyle@rc.com or 800-826-3579. The information in this update should not be considered legal advice. Consult your attorney before acting on anything contained herein.

© 2009 Robinson & Cole LLP

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission.