Katten
Katten Muchin Rosenman LLP

ClientAdvisory

The American Recovery and Reinvestment Act of 2009: Health Information Privacy and Security Provisions—Here We Go Again

February 26, 2009

On February 17, 2009, President Obama signed into law The American Recovery and Reinvestment Act of 2009 (the "Stimulus Act" or the "Act"), which will address the nation's economic uncertainties through various tax breaks and infrastructure investment projects. The Act includes almost $20 billion for the development of a nationwide health information technology ("HIT") infrastructure intended to, among other things, advance the adoption of electronic medical records, improve health care quality, reduce medical errors and improve care coordination.

The Stimulus Act also includes numerous provisions which modify and expand the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including requiring HIPAA-covered entities, business associates and other previously unregulated entities to modify their health information privacy and security policies, procedures and practices.

Health Information Technology for Economic and Clinical Health Act

Title XIII of the Stimulus Act, also known as the "Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act", addresses the promotion of HIT. Subtitle D of the HITECH Act expands the HIPAA Privacy Rule and Security Rule and includes other provisions which will require attention by health care organizations and other entities not previously impacted by HIPAA.

Highlights of the HITECH Act

Significant changes to be implemented by the Act include the following:

- Direct application of key Security Rule and Privacy Rule obligations to business associates and an expanded definition of persons and entities considered to be business associates
- Requiring covered entities and personal health record ("PHR") vendors to notify affected individuals and federal regulatory entities of security breaches involving an individual's "unsecured" protected health information ("PHI") or PHR identifiable health information, respectively
- Modifying and expanding the scope of the Privacy Rule (e.g., narrowing the scope of permitted marketing activities without individual authorization, modifying the minimum necessary rule, requiring a covered entity to agree to disclosure restriction requests, reviewing the definition of health care operation activities, expanding the scope of accounting disclosure obligations)
- Restricting the sale of PHI by covered entities without individual authorization
- Expanding the scope of penalties for unlawfully using and disclosing PHI, and the scope of individuals permitted to file claims for HIPAA violations to include state attorneys general, and also requiring the Secretary of Health and Human Services (the "Secretary") to establish a methodology for sharing a percentage of HIPAA civil monetary penalties and settlement amounts with aggrieved individuals
- Requiring the Secretary to conduct mandatory audits of covered entities and business associates

Direct Application of HIPAA Security Rule and Privacy Rule Provisions to Business Associates

Under current law, business associates are not directly regulated by HIPAA or its implementing regulations. Lacking statutory authority to directly regulate any person other than "covered entities" (i.e., health care providers that engage in a standard transaction, health plans and health clearinghouses), the Secretary addressed the disclosure of PHI to third-party vendors of covered entities by requiring the covered entities to enter into HIPAA-compliant business associate contracts with such persons and organizations. Thus, a business associate's HIPAA obligations are by contract and not by statute or law.

The Stimulus Act significantly changes that approach. HIPAA business associates will now be subject directly to many of the same Security Rule requirements as covered entities, meaning that business associates will need to implement the administrative, physical and technical safeguards required by 45 CFR Part 164, Subpart C. Business associates will also need to implement the requisite Security Rule policies and procedures required of covered entities.

Business associates will also be bound by the Privacy Rule and will be subject to the same civil monetary penalties and criminal penalties that are applicable to covered entities for Privacy Rule and Security Rule violations.

Effective as of February 17, 2009, the Act states specifically that organizations such as health information exchange organizations and regional health information exchange organizations that provide data transmission of PHI on behalf of a covered entity and that routinely require access to such information are business associates of the participating covered entities. Many such organizations had argued that they were mere conduits of PHI and, therefore, were not business associates of any covered entity participants or members.

Action Item: This is a significant expansion to the scope of the Privacy Rule and Security Rule. Like covered entities, business associates will need to implement a health information security program that comports with the standards set forth in the Security Rule. This will include a required risk analysis. Covered entities will also need to ensure the implementation of these obligations by their business associates, presumably through appropriate representations and warranties, which may necessitate the execution of business associate contract amendments or amended and restated business associate agreements. Further, covered entities that did not previously execute business associate contracts with health information exchange organizations in which they participate will need to execute such agreements.

Notification of Data Security Breach Required for Covered Entities, PHR Vendors and Other Non-Covered Entities

The current version of the Security Rule does not require covered entities to notify their patients, insureds or customers in the event of a security breach involving PHI. (Many states would, however, require such a notification depending upon the information involved.) Per the Stimulus Act, no later than 60 days after discovery of a breach or a suspected breach, covered entities would be required to notify individuals whose "unsecured" PHI has been or is reasonably believed by the covered entity to have been accessed, acquired or disclosed. There is no materiality standard regarding the type or scope of PHI involved.

"Unsecured PHI" is defined as PHI that is not secured through the use of a technology or methodology to be defined by the Secretary. Guidance from the Secretary on the matter is required within 60 days of enactment of the Stimulus Act. Until such time, PHI will be deemed secured if it is encrypted by a technology or methodology developed or endorsed by an ANSI accredited organization.

Business associates would also be required to notify covered entities of a security breach. Written notice of a data security breach to affected individuals would be required in all cases. The Secretary would also need to be notified of all security breaches (immediately in the case of a security breach involving 500 or more persons or annually via a log-book submission if less than 500 persons were involved). In cases involving 500 or more persons in a given state or media jurisdiction, notice to the media would also be required.

The required content of the notice is similar to that currently employed by many financial entities and organization alerting customers to a possible security breach or identity theft event (e.g., description of the event, types of unsecured PHI involved, steps that the person should take to mitigate potential harm, description of what actions the covered entity is taking to investigate, mitigate losses and protect against further breaches).

The Act also includes virtually identical data security breach notification requirements for vendors of PHRs. Because PHR vendors may not be HIPAA-covered entities, instead of notifying the Secretary of a breach of unsecured PHR identifiable health information, the Act requires the PHR vendor (and, via the PHR vendor, its third-party service providers) to notify the Federal Trade Commission ("FTC") (which, in turn, will notify the Secretary). Violations of these notification requirements by a PHR vendor will be treated as an unfair and deceptive act or practice in violation of the FTC Act.

The Stimulus Act specifies that the Secretary (and, in the case of security breaches involving PHRs, the FTC) shall publish interim final regulations implementing these notice provisions no later than 180 days after enactment of the Stimulus Act, to be effective 30 days after publication. Thus, assuming no publication delays, these provisions would be effective no later than September 2009.

Action Item: The Act establishes new federal security breach notice obligations that expand upon the current notice obligations imposed by many states following a data security breach. While these notice obligations are consistent with other federal initiatives intended to minimize the risk and consequences of identity theft, including medical identity theft (e.g., the FTC's Red Flag Rules to be effective as of May 1, 2009), the health care industry will need to implement policies and procedures to comply with the scope and requirement of the security breach notice obligations of the Act.

To avoid the security breach notice obligations for "unsecured" PHI imposed by the Act, covered entities may consider the cost and appropriateness of encrypting their electronic PHI (and the cost and appropriateness requiring its business associates to encrypt PHI), even when such PHI is "at rest." Further, even without regulatory guidance from the Secretary, covered entities may want to consider the appropriateness of implementing policies and procedures designed to notify their patients, insureds and customers in the event of a data security breach.

Restrictions on Disclosures of Certain PHI

Under the version of the Privacy Rule currently in effect, an individual may request that a covered entity restrict its uses and disclosure of PHI for treatment, payment and health care operation activities. However, the covered entity need not agree to such a request. The Act expands the scope of the Privacy Rule and specifies that a covered entity *must* comply with a restriction request if: (a) the disclosure is to a health plan for purposes of carrying out payment or health care operation activities, and (b) the PHI pertains solely to a health care item or service for which the health care provider has been paid in full out of pocket. Thus, if an insured individual elects to pay out-of-pocket for a health care product or service, that individual may request, and the covered health care provider must agree, not to disclose any PHI related to that product or service to the individual's health plan.

Action Item: Covered health care providers will need to implement policies and procedures to allow patients to restrict the disclosure of PHI to a health plan if the patient pays for the item or service out-of-pocket. One would presume that the patient will also need to be notified of this right via the provider's notice of privacy practices or otherwise. Health plans will also need to consider how this new disclosure restriction right might affect their underwriting activities.

Modifications to the Minimum Necessary Rule

Aside from certain uses and disclosures (e.g., disclosures for treatment activities), the Privacy Rule specifies that a covered entity must limit its use and disclosure of PHI to the "minimum necessary" amount to accomplish the intended purpose. The Stimulus Act obligates the Secretary to publish guidance on what constitutes the minimum necessary amount of PHI within 18 months of enactment of the Act (i.e., by August 2010). In doing so, the Stimulus Act provides specifically that the Secretary shall take into account information "necessary to improve patient outcomes and to detect, prevent and manage chronic disease." Whether said guidance (based upon the Stimulus Act's mandate to account and allow for outcome improvements and disease detection, prevention and management) leads to an expanded interpretation of the minimum necessary amount remains to be seen.

Pending issuance of the Secretary's minimum necessary guidance, the Stimulus Act specifies that a covered entity shall be deemed to have satisfied the minimum necessary rule on use and disclosure of PHI *only if* the covered entity limits the PHI: (1) " to the extent practicable" to a limited data set ("LDS") of PHI, or (2) to the minimum necessary amount of PHI to accomplish the intended purpose (in the case of a disclosure, said determination to be made by the disclosing party). Although somewhat ambiguous, the strong implication is that an LDS of PHI becomes the minimum necessary default

standard (i.e., covered entities must use and disclose an LDS to the extent practicable and, *only if not practicable*, use and disclose the minimum amount of PHI necessary to accomplish the purpose). Implicit in this interim default standard is an expansion of the current scope of permissible uses for an LDS—presently restricted to research, public health and health care operation activities—to include other permitted uses and disclosures of PHI under the Privacy Rule (e.g., payment).

Action Item: The practical impact of the interim LDS default standard is troublesome for covered entities. Pending guidance from the Secretary, will covered entities need to revise (on a temporary basis only to revise again once minimum necessary guidance is issued by the Secretary) their policies, procedures and practices regarding the use and disclosure of PHI (for non-treatment activities)? And, if so, at what cost? When is use and disclosure of an LDS "practicable"? Who decides? Does cost factor into the practicality evaluation?

Ultimately, many covered entities may determine that an LDS is impractical in some situations and determine that an expanded set of PHI is the most appropriate and minimum necessary.

Accounting of Disclosures for Covered Entities Using EHRs and Access to PHI Maintained in an EHR

Currently, covered entities need not provide an accounting of disclosures related to treatment, payment and health care operation activities. The Stimulus Act eliminates that exception for disclosures made through an electronic health record ("EHR"). An individual will have a right to receive an accounting of disclosures made by a covered entity through an EHR for treatment, payment, and health care operations for a three-year period prior to the request. An individual is otherwise entitled to an accounting of disclosures made during the six-year period prior to the individual's request.

To effectuate this provision, the Secretary must publish regulations within 18 months of the date that the Secretary adopts standards for technologies that, as part of a qualified EHR, will allow for an accounting of electronic disclosures of PHI. Covered entities need only account for electronic disclosures of PHI for treatment, payment and health care operation activities which they make. Covered entities may also charge a reasonable fee for such accountings, but the fee cannot exceed the covered entity's labor costs in responding to the request.

Because of the significance of this expanded disclosure accounting obligation, the Act defers its effective date.

- For covered entities with EHRs as of January 1, 2009, the disclosure accounting obligation is effective for disclosures made on or after January 1, 2014.
- For covered entities that implement EHRs after January 1, 2009, the disclosure accounting obligation is effective for disclosures made on or after the later of January 1, 2011, or the date on which the covered entity implements an EHR.
- Furthermore, the Secretary is permitted to delay the aforementioned effective dates, but in no event may the effective date be later than January 1, 2018 (for covered entities with EHRs as of January 1, 2009), or January 1, 2014 (for covered entities that implement EHRs after January 1, 2009).

The Stimulus Act also affords individuals requesting access to PHI maintained in an EHR the right to obtain a copy of any such PHI in an electronic format. The Act provides further that the fee that a covered entity may charge an individual for an electronic copy of his/her PHI is limited to the covered entity's "labor costs" in responding to the request.

Action Item: Implementation of the disclosure accounting and electronic access obligations is likely to be a significant undertaking for covered entities with EHRs, and vendors that develop and license EHR software. Even with the delayed effective dates, covered entities and their software vendors should begin to plan for this obligation as soon as possible.

Health Care Operations Redefined and Marketing Communications

The Stimulus Act seeks to narrow the scope and definition of "health care operations" under the Privacy Rule. Not later than 18 months from the effective date of the Act, the Secretary is obligated to review the definition of health care operations and, with the exception of activities described in paragraph (1) of the definition of health care operations at 45 CFR 164.501 (e.g., quality assurance and improvement activities), "to the extent appropriate, eliminate by regulation activities that can reasonably and efficiently be conducted through the use of information that can be de-identified or that should require a valid authorization for use and disclosure." If the Secretary elects to modify or clarify the definition and

scope of health care operations, the effective date of those changes shall not be sooner than 24 months after the enactment date of the Act (i.e., February 2011).

The Act also reaffirms that marketing is not a health care operation, unless it falls within one of the existing exceptions (i.e., communicating about health products or services, treatment alternatives or case management and coordination). However, the Stimulus Act also narrows the scope of permitted/excepted marketing communications under the Privacy Rule by providing that an otherwise excepted marketing communication will not be considered to be a health care operation activity (and, therefore, individual authorization will be required prior to use and disclosure of PHI) if the covered entity receives any remuneration (directly or indirectly) in exchange for those communications. These changes are to be effective 12 months from the enactment date of the Act.

Action Item: Covered entities will need to revise their policies, procedures and practices to reflect this change in the definition of marketing and monitor potential future changes to the definition of health care operations by the Secretary.

Restrictions on the Sale of Health Information

The Privacy Rule regulates the use and disclosure of PHI. So long as a disclosure is otherwise permitted by the Privacy Rule (e.g., an LDS of PHI for research), the Privacy Rule does not regulate the sale of PHI. However, there has been recent discussion and debate concerning the ownership and sale of patient-identifiable information. *See, e.g., IMS Health Inc. v. Ayotte*, 2008 WL 4911262 (1st Cir., Nov. 18, 2008).

Perhaps in response to such discussion and debate, the Stimulus Act states, with certain defined exceptions, that a covered entity and its business associates may not receive any remuneration or charge for any PHI *unless* the covered entity has received specific authorization from an individual that his/her PHI can be further exchanged for remuneration. Notable exceptions to the prohibition against the exchange of PHI for remuneration without individual authorization include:

- remuneration related to the exchange of PHI for research or public health activities (as such terms are defined by the Privacy Rule);
- remuneration related to the exchange of PHI for treatment;
- PHI exchanged in connection with the sale, transfer or merger of a covered entity;
- remuneration provided to a business associate in connection with the business associate's services to the covered entity;
- remuneration provided in connection with the provision of a copy of an individual's PHI pursuant to 45 CFR 164.524; and
- the purpose of the remuneration exchange is otherwise determined by the Secretary to be "necessary and appropriate."

In order to implement this provision, Congress requires the Secretary to promulgate regulations not later than 18 months after enactment of the Stimulus Act (i.e., by August 2010). The regulations would become effective no later than six months after promulgation of the final rules. In promulgating those regulations, Congress requires the Secretary to:

- evaluate the impact on research and public health activities if the remuneration permitted under the research/public health exception described above is limited to the costs of preparing and transmitting the data; and
- based upon that evaluation, determine whether that exception should be further limited by restricting the price to be charged to said data preparation and transmittal costs.

Action Item: This is a potentially significant provision for many covered entities. Health care provider organizations and systems (and their various vendors) are beginning to recognize the economic value of patient information data bases. To the extent covered health care provider entities seek to continue to license the use of components of said patient databases to third parties, such data may need to be de-identified, as an LDS may no longer be appropriate. An LDS is "protected health information that excludes [certain] direct identifiers." 45 C.F.R. §164.514 (e)(2). Read literally, the Act precludes the sale of an LDS *of PHI* for non-research or non-public health purposes (i.e., a health care operation activity) without patient authorization (a practical impossibility for each sale of PHI). As an example, many covered health care providers currently furnish an LDS of PHI to their product manufacturers and suppliers in exchange for negotiated rebates

and discounts (a permitted health care operation activity under the Privacy Rule). Those practices may need to be modified to require only the disclosure of de-identified health information to said manufacturers and suppliers.

Psychotherapy Notes

The Act requires the Secretary to amend the definition of "psychotherapy notes" to include "test data that is related to direct responses, scores, items, forms, protocols, manuals, or other materials that are part of a mental health evaluation, as determined by the mental health professional providing treatment or evaluation."

Penalties and Enforcement

The Stimulus Act includes a number of clarifications and modifications related to the enforcement of the Privacy Rule and Security Rule requirements:

- The Act clarifies that individual persons can be held criminally responsible for unlawful receipt and disclosure of PHI. This appears to be in response to a memorandum opinion issued by the Department of Justice ("DOJ") on June 1, 2005, following a well-publicized criminal indictment and plea of an employee of a Seattle-based health care provider for having wrongfully obtained and sold PHI. The DOJ opinion indicated that, except in unusual circumstances, the DOJ did not believe that individual persons could be criminally prosecuted for Privacy Rule violations, as HIPAA governed only the conduct of covered entities. That interpretation was widely criticized by privacy advocates and many current and former United States Attorneys.
- Effective February 17, 2011, the Act requires the Secretary to impose civil money penalties for "willful neglect" of the Privacy Rule and Security Rule requirements. The Secretary is obligated to promulgate regulations to implement this change no later than 18 months after enactment of the Act.
- The Act requires all civil money penalties and settlement amounts collected with respect to the enforcement of the Privacy Rule or Security Rule to be transferred to the Office for Civil Rights ("OCR") of the United States Department of Health and Human Services to further assist with such enforcement activities.
- Not later than 18 months after its enactment, the Act requires the Government Accountability Office ("GAO") to recommend to the Secretary a methodology for sharing civil money penalties and settlement amounts with individuals who may be harmed by an act that constitutes a violation of the Privacy Rule or Security Rule. Based upon those recommendations, the Act requires the Secretary to publish regulations (not later than three years after enactment of the Act) setting forth such a methodology.
- As of its enactment date, the Act implements a tiered civil money penalty provision for Privacy Rule and Security Rule violations, as follows:
  - Unknowing violations—at least $100 per violation, not to exceed $25,000 in a calendar year
  - Violations due to reasonable cause and not willful neglect—at least $1,000 per violation, not to exceed $100,000 in a calendar year
  - Violations due to willful neglect—at least $10,000 per violation, not to exceed $250,000 in a calendar year, except that if the violation is not corrected within 30 days of the date the person knew or should have known of the violation, the penalties increase to at least $50,000 per violation, not to exceed $1.5 million in a calendar year
- For Privacy Rule and Security Rule violations occurring after the date of enactment of the Act, unless a federal action is pending, the Act affords the Attorney General of each state the authority to file a civil action in a district court of the United States of appropriate jurisdiction on behalf of the residents of such state to enjoin any person from violating the Privacy Rule or Security Rule or to obtain damages on behalf of such state's residents. Statutory damages are determined by multiplying the number of violations by up to $100, not to exceed $25,000 for all violations of an identical requirement per calendar year. The court may also award reasonable attorney fees to the state. Except where such notice is not feasible, the state shall serve prior written notice to the Secretary of any such action, and the Secretary shall have the right to intervene.
- The Act specifies that, notwithstanding any of the enforcement provisions and penalties set forth in the Act, OCR retains the discretionary authority to continue to use corrective action without a penalty in cases where the person did not know (and by exercising reasonable due diligence would not have known) of the violation involved.

Action Item: The Act creates significant new tools for the enforcement of HIPAA and the HIPAA Privacy Rule and Security Rule. Those tools will undoubtedly lead to more enforcement actions. Covered entities and business associates will need to re-examine their existing policies and procedures to ensure compliance with current law and to revise as necessary to comply with the Act. Privacy, security and compliance officers must also be prepared to address compliance issues, audits and investigations.

De-identification of Health Information

Within 12 months of enactment, the Act requires the Secretary to issue guidance on "how best to implement the requirements for the de-identification of protected health information" under the Privacy Rule. It is unclear how this best practice guidance will substantively modify, if at all, the current methodologies for the de-identification of PHI (i.e., safe harbor and statistician opinion) .

Compliance Audits and Reports

The Act requires the Secretary to conduct periodic audits to ensure that covered entities and business associates act in and are in compliance with the Privacy Rule and Security Rule. The Act also requires the Secretary to file annual reports with Congress concerning complaints of alleged violations of law relating to the privacy and security of health information that are received by the Secretary during that year, which report shall be publicly available.

Within 12 months of enactment, the Act also requires:

- the Secretary, in consultation with the FTC, to conduct a study and to submit a report, including recommendations, on privacy and security requirements for entities that are not covered entities or business associates;
- the GAO to report to Congress on best practices related to disclosures of PHI among health care providers for treatment purposes; and
- the GAO to issue a report to Congress and the Secretary on the impact on the Act's privacy and security provisions on health insurance premiums and overall health care costs.

If you have any questions about the data privacy and security provisions of the HITECH Act, please contact Brian Annulis at 312.902.5473 or brian.annulis@kattenlaw.com.

Katten

Katten Muchin Rosenman LLP www.kattenlaw.com

CHARLOTTE CHICAGO IRVING LONDON LOS ANGELES NEW YORK PALO ALTO WASHINGTON, DC

Katten Muchin Rosenman LLP is an Illinois limited liability partnership including professional corporations that has elected to be governed by the Illinois Uniform Partnership Act (1997). London affiliate: Katten Muchin Rosenman Cornish LLP.

2/26/09