ReedSmith

lshi

Life Sciences Health Industry Alert

If you have questions or would like additional information on the material covered in this Alert, please contact the author:

Brad M. Rostolsky
Associate, Philadelphia
+1 215 851 8195
rostolsky@reedsmith.com

Gina M. Cavalier
Partner, Washington, D.C.
+1 202 414 9288
gcavalier@reedsmith.com

Debra L. Hutchings
Associate, Chicago
+1 312 207 3884
dhutchings@reedsmith.com

Kerry A. Kearney
Partner, Pittsburgh
+1 412 288 3046
kkearney@reedsmith.com

Mark S. Melodia
Partner, Princeton
+1 609 520 6015
mmelodia@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Client Alert 09-059

March 2009

reedsmith.com

HIPAA Privacy and Security Changes in the American Recovery and Reinvestment Act

On Feb. 17, 2009, President Obama signed into law H.R. 1, the American Recovery and Reinvestment Act (the "ARRA").[1] This memorandum outlines significant changes and additions to the landscape of federal privacy and security law set forth in Subtitle D of the ARRA. In general, the privacy and security portions of the ARRA become effective 12 months after the enactment of the ARRA, which is approximately February 2010. It is also important to note that the ARRA directs the Secretary of the U.S. Department of Health & Human Services ("HHS") to amend the HIPAA Privacy and Security Rules to implement the legislative changes. As such, the effective dates associated with the rulemaking process will vary.

A. Applicability of HIPAA Security and Privacy Rules Extended to Business Associates

1. Security Rule

The HIPAA Security Rule's information safeguards are not new considerations for Business Associates. Business Associate Agreements contractually obligate Business Associates to implement administrative, physical, and technical safeguards to reasonably and appropriately protect electronic protected health information that the Business Associate creates or maintains on behalf of a Covered Entity. The ARRA, however, changes the fundamental framework of the Security Rule in this regard. Specifically, Business Associates are now required to directly comply with the Security Rule's provisions on administrative, physical, and technical safeguards, as well as to develop implementing policies and procedures. As a practical matter, however, it is unclear whether these provisions only apply vis-à-vis the protected health information created or received from a Covered Entity, or whether they implicate other information of the Business Associate.

As a means to assist Business Associates (as well as Covered Entities) with effectively addressing the requirements of the Security Rule, HHS is required to publish annual guidance on "the most effective and appropriate technical safeguards for use in carrying out" the requirements of the Security Rule. Additionally, the ARRA requires that Business Associate Agreements reflect the new direct obligations of Business Associates. Finally, adding enforcement teeth, the ARRA provides that Business Associates will be subject to civil and criminal penalties for violating the Security Rule.

2. Privacy Rule

The ARRA requires a Business Associate that "obtains or creates protected health information pursuant to a written contract" to take direct responsibility for its uses and disclosures of protected health information. As a result of the new legislation, and regardless of the contractual obligations of a Business Associate Agreement, the manner in which Business Associates approach Privacy Rule requirements and obligations has been significantly altered, although the extent of these changes will not be clear until regulations are promulgated.

At a minimum, it is clear that Business Associates that violate the Privacy Rule obligations set forth in their Business Associate Agreements will be subject to HIPAA's civil and criminal enforcement provisions. The statutory language also appears to require a Business Associate to take reasonable steps to cure a Covered Entity's violation of a Business Associate Agreement if the Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material breach or violation of the Covered Entity's obligation under the Business Associate Agreement. If cure is not possible, and termination of the Business Associate is not feasible, then the Business Associate must report the problem to HHS.

It is likely that the requirement that Business Associates' new privacy and security obligations be reflected in Business Associate Agreements will, de facto, require the amendment of current Business Associate Agreements. Although the standard language typically found in Business

Associate Agreements may be sufficient to address some of the increased privacy and security requirements, it may behoove Covered Entities and Business Associates to review their current Business Associate Agreements. Amendments to current Business Associate Agreements will enable the parties to ensure that both the Privacy and Security Rules are properly and thoroughly addressed. Furthermore, it seems likely that Covered Entities will want the security breach notification requirements discussed below to be set forth in detail in Business Associate Agreements.

3. Definition of Business Associate Expanded

The ARRA expands the definition of "Business Associate" to any organization that, with respect to a Covered Entity, provides data transmission of protected health information to a Covered Entity (or its Business Associate) if the organization requires routine access to the protected health information. Examples include a Health Information Exchange Organization, a Regional Health Information Organization, an E-prescribing Gateway, or a Vendor of Personal Health Records. (ARRA provisions related to Vendors of Personal Health Records are described below.) The new universe of entities will be treated as "Business Associates," and must, among other things, enter into a Business Associate Agreement with Covered Entities.

B. Notification Standards for Breaches of "Unsecured" Protected Health Information

1. Covered Entities

Much like the security breach notification laws of many states, the ARRA imposes significant breach notification obligations on a Covered Entity that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information." Thus, any such Covered Entity that knows or should reasonably have known that protected health information has been acquired, accessed, used, or disclosed without authorization, must provide notice of the breach to individuals and designated entities within a prescribed period of time.

The ARRA includes detailed requirements regarding when, how, and to whom notifications of a breach must be provided, but, generally, the notifications must be provided to the individual about whom the information pertains without unreasonable delay (and, in any event, no later than within 60 days of discovery of the breach). In addition to notifying the individuals, notification must always be provided to HHS (immediately if the breach involves more than 500 individuals, or annually otherwise), and, depending on the scope or severity of the breach, to prominent media outlets serving the respective state or jurisdiction. The one exception to a Covered Entity's obligation to provide a security breach notification is if a law enforcement official determines that such a notification would impede a criminal investigation or cause damage to national security. HHS will maintain a website that identifies Covered Entities involved in a breach of unsecured protected health information for more than 500 individuals.

The ARRA defines unsecured protected health information to mean "protected health information that is not secured through the use of a technology or methodology specified by the Secretary [of HHS] in" guidance that will be issued no later than 60 days after the enactment of the ARRA. In case the aforementioned guidance is not issued by HHS on the date promised, the ARRA provides the following default definition of unsecured protected health information, which appears to essentially require encryption – "protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute."

No later than 180 days after the enactment of the ARRA (approximately August 2009), HHS shall promulgate interim final regulations. The security breach notification provisions of the ARRA shall be effective 30 days after the publication of these interim final regulations (approximately September 2009). Note: This is sooner than the effective date for the ARRA generally.

2. Business Associates

The breach notification requirements extend to Business Associates insofar as Business Associates must report discovered breaches of unsecured protected health information to the Covered Entity following a Business Associate's discovery of a breach. If a Business Associate fails to provide the required notice in a timely fashion, the Business Associate may be subject to direct enforcement and penalties. Notification from a Business Associate must include the identification of each individual about whom the breached information pertains. Covered Entities will likely include specific notification timing requirements in Business Associate Agreements.

3. Vendors of Personal Health Records

The ARRA also imposes breach notification requirements on "Vendors of Personal Health Records." Under the ARRA, a Vendor of Personal Health Records is any entity "other than a covered entity [as defined in the HIPAA regulations] that offers or maintains a personal health record." The term "personal health record" is defined to be "an electronic record of [individually identifiable health information (as defined in the Social Security Act)] on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or for the individual."

Vendors of Personal Health Records must notify the individual about whom the information pertains, as well as the Federal Trade Commission ("FTC") (which will in turn notify HHS) upon discovery of a breach of security with respect to the individually identifiable health information that is in a personal health record. The ARRA defines "breach of security" to mean any acquisition of the aforementioned information without the authorization of the individual to whom the information pertains. Third party service providers engaged by Vendors of Personal Health Records are treated similarly to Business Associates, and must notify the vendor of a breach of security.

For Vendors of Personal Health Records and third-party service providers, the requirements regarding when and how they must provide notifications of a breach of security are the same as for Covered Entities and Business Associates, respectively. A Vendor of Personal Health Records or third-party service provider's violation of the notification requirements shall be considered an unfair and deceptive act or practice in violation of FTC regulations.

These provisions are intended to be temporary and will sunset if Congress enacts new legislation establishing specific security breach notification requirements for entities that are not Covered Entities or Business Associates under HIPAA. The FTC is required to promulgate implementing regulations within 180 days of the enactment of the ARRA (approximately August 2009), which will likely clarify the definitions and requirements set forth in the ARRA.

C. Enhanced Privacy Guidance and Education Initiative

Within six months after the enactment of the ARRA (approximately August 2009), HHS is required to designate an individual in each HHS regional office 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 protected health information." Additionally, within one year after the enactment of the ARRA, the HHS Office for Civil Rights is required to develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information.

D. Obligations Related to Electronic Health Records

1. Accounting of Protected Information Stored in Electronic Health Records

Although under the HIPAA Privacy Rule, Covered Entities are not required to account for uses and disclosures of protected health information for the purpose of treatment, payment, and health care operations, the ARRA specifically eliminates this exception for Covered Entities that use or maintain "electronic health records." The ARRA defines an "electronic health record" to mean "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

A Covered Entity must provide the new, broader, accounting upon request. For disclosures made by a Covered Entity's Business Associates, however, the Covered Entity may provide an individual with a list of the Business Associates. If an individual is provided such a list of Business Associates, then the Business Associates must provide the accounting to the individual upon request from the individual. Accountings made by Covered Entities and Business Associates that use and maintain electronic health records must cover a period of three years (as opposed to the six-year period required under HIPAA).

These accounting provisions are effective as follows:

- For Covered Entities, insofar as they acquired an electronic health record as of Jan. 1, 2009, the accounting requirement applies to disclosures made on or after Jan. 14, 2014.
- For Covered Entities insofar as they acquire an electronic health record after Jan. 1, 2009, the provision will be effective for disclosures on the later of Jan. 1, 2011, or the date upon which the entity acquires the electronic health record.

- HHS can impose a later effective date, but it can be no later than 2016 for the Covered Entities with an electronic health record as of Jan. 1, 2009, and 2013 for all other Covered Entities with an electronic health record.

2. Access to Protected Health Information in Electronic Format

Expanding on the Privacy Rule's access provisions, Covered Entities that use or maintain an electronic health record with respect to the protected health information of an individual must, per ARRA, provide access to such information by producing an electronic copy to the individual (or a recipient designated by the individual). Individuals making such a request may only be charged for a Covered Entity's labor costs associated with providing the requested information.

3. Sale of Electronic Health Records or Protected Health Information

The ARRA provides that a Covered Entity or Business Associate cannot directly or indirectly receive remuneration in exchange for an individual's protected health information (including such information stored in an electronic health record) except pursuant to a valid HIPAA authorization that specifies the extent to which the recipient may engage in further exchanges of the individual's information.

This prohibition does not apply to the exchange of the information if the purpose for the exchange is one of the following:

- Public health activities, as defined by the Privacy Rule (45 C.F.R. § 164.512(b))
- Research purposes (as defined in 45 C.F.R. §§ 164.501, 164.512(i)), subject to limitations on the remuneration
- Treatment, unless HHS determines otherwise
- Transfers in connection with the sale or merger of a Covered Entity
- Remuneration that is paid by the Covered Entity to a Business Associate related to the Business Associate's services as to the exchange of protected health information
- Providing an individual with a copy of the individual's protected health information
- Other situations, as determined by HHS

HHS is required to promulgate regulations implementing these provisions no later than 18 months after the enactment of the ARRA (approximately August 2010). Furthermore, this provision of the ARRA applies only to an exchange of protected health information that occurs at least six months after the regulations have been released.

E. Enhanced Ability of Individuals to Control Protected Health Information

1. Requested Restrictions on or Disclosures of Protected Health Information

Prior to the enactment of the ARRA, a Covered Entity was not required to grant an individual's request to limit the use and disclosure of protected health information to carry out treatment, payment, or health care operations. The ARRA, however, requires Covered Entities to comply with an individual's request for such restrictions on disclosure if:

- The disclosure is made to a health plan for the purposes of carrying out payment or health care operations (unless the use or disclosure is required by law)
- The protected health information at issue pertains only to a health care item or service for which the individual pays (1) out-of-pocket, and (2) in full.

2. Minimum Necessary Standard Further Explained

Under the Privacy Rule, a Covered Entity's use and disclosure of protected health information for purposes other than treatment, payment, and health care operations must be limited to the "minimum necessary" amount needed to accomplish the underlying purpose of the use or disclosure. To provide assistance to Covered Entities in this regard, the ARRA directs HHS to issue guidance on what constitutes "minimum necessary" no later than 18 months after the enactment of the ARRA. Until the release of this guidance, the ARRA provides that uses and disclosures unrelated to treatment, payment, or health care operations must be in the form of a limited data set (as defined by the Privacy Rule), unless a Covered Entity (or Business Associate) determines that a limited data set is not "practicable" for a particular use or disclosure, in which case the "minimum necessary" standard still applies.

3. Marketing and Fund-Raising Communications

The ARRA contains new restrictions on marketing communications. Specifically, marketing communications to an individual from a Covered Entity or Business Associate that were previously considered "health care operations" (and therefore not curtailed by the Privacy Rule) are no longer considered health care operations (and therefore no longer exempt from the Privacy Rule's general prohibition against disclosure) if the Covered Entity or Business Associate receives or has received direct or indirect remuneration (as defined under federal fraud and abuse regulations) for making the communication, except where:

- The communication describes a drug or biologic that is currently prescribed for the recipient, and the remuneration received by the Covered Entity in exchange for the information is "reasonable" (as will be defined by HHS)
- The communication is made by the Covered Entity based on a valid HIPAA authorization
- The communication is made by a Business Associate of the Covered Entity in accordance with a written Business Associate Agreement

Although fund-raising communications are still considered "health care operations," such communications must clearly and conspicuously provide individuals with an opportunity to opt-out of receiving further fund-raising communications. The decision by an individual to opt-out shall be considered a revocation of authorization under HIPAA.

F. Continued Focus on Enforcement Activities

Building on recent enforcement actions (settlements and informal compliance agreements) from the Office of Civil Rights and the Centers for Medicare and Medicaid Services, the ARRA amends the relevant enforcement provisions of HIPAA by, among other things, requiring HHS to "formally investigate any complaint of a violation of [the Privacy and Security provisions of the ARRA] if a preliminary investigation of the facts of the complaint indicate [that] such a possible violation [is] due to willful neglect." Notwithstanding this heightened focus on enforcement, the ARRA specifically permits the Office for Civil Rights to utilize corrective action without penalty as a means to address civil infractions of the Privacy Rule.

Except as separately provided in the ARRA, the amendments made to enforcement provisions shall be effective 24 months after the enactment of the ARRA (approximately February 2011).

1. State Attorneys General Can Initiate Federal Action for HIPAA Violations on behalf of State Residents

Furthermore, the ARRA authorizes state Attorneys General to initiate civil actions in federal court (for injunctive relief or monetary damages) on behalf of a state resident when the Attorney General reasonably believes that the resident's interests have been threatened or adversely affected by a person or entity that violates HIPAA. Additionally, the court may award the costs of the action and reasonable attorney fees to the state. Prior to bringing any such claim, a state Attorney General must provide HHS with prior written notice of intent to file the action, after which HHS may intervene in the action. If HHS brings a HIPAA action against a person, then state Attorneys General may not bring an action against the person relative to the same HIPAA violation.

2. Enforcement Clarification Regarding Individuals

The ARRA clarifies a point of confusion regarding the criminal enforcement of individuals for the wrongful access or disclosure of protected health information under HIPAA. The ARRA makes it clear that individuals (who are not Covered Entities, but who may be employees of Covered Entities) fall within HIPAA's enforcement purview.

3. Increased to Civil Monetary Penalties

With regard to civil monetary penalties, the ARRA replaces the manner in which such penalties are determined with a new tiered approach:

- Unknown violations (i.e., if a person did not know, and by exercising reasonable due diligence would not have known, that a violation occurred): 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.

- Violations as a result of reasonable cause and not because of willful neglect: The penalty shall be at least $1,000 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.
- Violations as a result of willful neglect (and the violations have been 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.
- Violations because of willful neglect (and that have not been 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.

Also note that, within three years of the enactment of the ARRA, HHS is required to publish regulations that establish a methodology that distributes a portion of collected civil monetary penalties to the individuals harmed by a Covered Entity's act of willful neglect. The application of this new tiered approach to civil monetary penalties applies to violations that occur after the date of enactment of the ARRA.

---

1 P.L. No. 111-5. The text of the Act and the accompanying conference report are available at http://thomas.loc.gov/home/approp/app09.html#h1.

About Reed Smith

Reed Smith is one of the 15 largest law firms in the world, with more than 1,700 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East.

Founded in 1877, the firm represents leading international businesses from Fortune 100 corporations to mid-market and emerging enterprises. Its attorneys provide litigation services in multi-jurisdictional matters and other high stake disputes, deliver regulatory counsel, and execute the full range of strategic domestic and cross-border transactions.

Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising and media, shipping, energy, trade and commodities, real estate, manufacturing, and education. For more information, visit **reedsmith.com**