

UNDERSTANDING THE STIMULUS PACKAGE'S CHANGES TO HIPAA'S PRIVACY PROVISIONS

By: Susan E. Gindin¹

On February 17, 2009, President Barack Obama signed the stimulus package (the American Recovery and Reinvestment Act of 2009 ("ARRA")) into law. Among other provisions of the massive law, ARRA contains \$19 billion in incentives for advancement of a nationwide health information infrastructure and adoption of electronic medical records, along with far-reaching changes to HIPAA's privacy and security provisions.

Although most HIPAA changes take effect on February 17, 2010, others take effect more quickly, and covered entities, business associates, and entities which provide services involving the handling of personal health information ("PHI") should be taking action now to comply with the changes in the law and to ensure that they have effective PHI handling processes in place.

Following are some of ARRA's major changes to HIPAA:

HIPAA's Privacy and Security Provisions Now Apply Directly to Business Associates

Under the current law, covered entities are required to enter into agreements with business associates ensuring compliance with HIPAA's requirements, and covered entities are responsible for ensuring their business associates comply with HIPAA through the terms of the agreements. While business associates are liable to the covered entities for breach of the agreements, they have not been directly liable for HIPAA violations under the current law.

ARRA changes that. While covered entities will still need to ensure that business associates comply with the business associate agreements, business associates will be directly liable under much of HIPAA, subject to the same civil and criminal penalties as covered entities, and directly liable to the Department of Health and Human Services ("HHS"), or to state attorneys general, for failure to comply.

Definition of Business Associate Has Been Expanded

ARRA expands the definition of business associate to include entities that provide data transmission of PHI to a covered entity or its business associate and require routine access to such PHI, for example, health information exchange organizations, regional health information organizations, e-prescribing gateways, or vendors that contract with a covered entity to allow that covered entity to offer a personal health record ("PHR") to patients. Therefore, these "new" business associates must enter business associate agreements with covered entities and they are subject to the same penalties as covered entities.

Data Breach Notification Requirements

To give affected individuals notice that their PHI may have been accessed by unauthorized parties, ARRA requires that covered entities, business associates, and PHR service providers provide notice for breach of PHI data in any format—paper as well as electronic.

¹ © 2009 Isaacson Rosenbaum P.C. Prepared by Susan E. Gindin. Susan is Of Counsel to the firm and specializes in data privacy and security, intellectual property and online law, advertising and contest law.

Covered entities must notify every individual potentially affected by a breach involving "unsecured" PHI within 60 days of discovery. They must also notify HHS, and in breaches involving 500 individuals or more, the media. Business associates are required to inform the covered entity about breaches within their organizations, and PHR vendors must also notify affected individuals and the Federal Trade Commission ("FTC"). ARRA prescribes the exact content of the notifications and additional requirements.

Notification must be made by letter or by e-mail if the individual has expressed a preference to receive notices electronically. Substitute forms of notice such as a conspicuous website posting are permitted when the covered entity does not have adequate contact information for at least 10 affected individuals. If more than 500 individuals in a geographic area are affected, notice must be provided to "prominent media outlets" in that geographic area. Notice must also be provided to HHS but if there are less than 500 individuals affected, the covered entity may provide this information to HHS as part of an annual report. If more than 500 individuals are affected, HHS will list the breach on its website.

The content of the notice must include (1) a brief description of the breach, including the date of the breach and the date it was discovered; (2) a description of the types of unsecured PHI involved in the breach (e.g., social security number, date of birth, etc.); (3) steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of actions the covered entity is taking to investigate and mitigate losses from the breach, and prevent further breaches; and (5) contact information in case there are additional questions.

A key point is that such notification is required only for *unsecured* PHI which is defined as PHI that is not secured through a technology or methodology that HHS states renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals. ARRA directs HHS within 60 days of ARRA's enactment to identify technologies to ensure that information is secure. Therefore, covered entities which use the protocols that HHS specifies can avoid the extensive and expensive breach notification requirements.

HHS and the FTC are directed to issue interim final regulations implementing the security breach notification requirements within 180 days of ARRA's enactment, with the requirements becoming effective 30 days after the publication of such regulations.

Enhanced Patient Rights to Their PHI Records, Further Limitations in Use and Disclosures of PHI

The new law expands patient rights with regard to access to their PHI and the covered entity's accounting of disclosures of their PHI, and also with regard to restricting disclosure in certain situations. Further, ARRA strengthens HIPAA's requirements that covered entities use and disclose the "minimum necessary" PHI to accomplish the intended purpose of the use or disclosure. ARRA specifies the minimum necessary as a "limited data set," which is PHI that excludes a long list of direct identifiers of the patient or of relatives, employers, or household members (for example, address, photo, social security number). These requirements will be replaced by "minimum necessary" guidance HHS is charged with issuing within 18 months of ARRA's enactment.

Further Limitations in Marketing and Fundraising

ARRA strengthens HIPAA restrictions on use of PHI for marketing purposes and also contact for fundraising purposes. First, the current law requires that before marketing to a patient, the covered entity must obtain patient authorization, and the authorization must disclose the fact that the covered entity is receiving direct or indirect remuneration from a third party, if applicable. However, under the current law, there is a broad carve-out for a wide variety of activities that are

defined as “health care operations,” including “contacting of health care providers and patients with information about treatment alternatives.” Under the new law, authorization must be obtained before communicating for marketing purposes unless the communication pertains only to a drug or biologic that is currently prescribed for the patient and the payment the covered entity receives is “reasonable in amount” (to be further defined by the HHS by regulation).

Also, ARRA provides that without valid authorization from the patient, entities may not receive remuneration for PHI (for example, from a drug company wanting the covered entity to send the communication) except for certain activities (for example, public health activities, research, treatment, certain business management and administrative activities of the entity or contractual obligations with a business associate, or to cover the cost of providing the individual’s PHI record to the individual).

In addition, the law requires that all fundraising communications must give the recipient an opportunity (presented in a clear and conspicuous manner) to opt not to receive any further fundraising communication.

Enhanced Enforcement Regime

ARRA makes a number of significant changes to HIPAA penalties and enforcement. The civil penalties include a new tiered civil monetary penalty structure with fines of up to \$50,000 per violation with an annual cap of \$1,500,000. ARRA also clarifies that the HIPAA criminal penalty provisions (fines of up to \$250,000 and 10 years imprisonment per violation) apply to employees and other individuals (not just covered entities) who use or disclose PHI obtained or disclosed without authorization.

ARRA also adds requirements and penalties for entities violating HIPAA through “willful neglect.” HHS must institute regulations that impose a mandatory civil penalty for any HIPAA violation due to “willful neglect.” Also, HHS must formally investigate any complaint of a HIPAA violation if a preliminary investigation of the facts of the complaint indicates a possible violation of HIPAA due to willful neglect.

Further, ARRA allows state attorneys general to enforce HIPAA privacy and security requirements through civil actions against those who violate HIPAA privacy or security requirements. State attorneys general may obtain injunctive relief, attorneys’ fees, and statutory damages of \$100 for each violation with an annual cap of \$25,000 for repeat violations.

ARRA also requires HHS to periodically audit covered entities and business associates to ensure compliance with HIPAA (rather than investigate only upon receipt of complaints), and HHS is charged with adopting regulations under which an individual who is harmed by a HIPAA privacy or security breach may receive a percentage of any civil monetary penalty or monetary settlement.

What This Means For You

ARRA will have a significant impact on all entities which handle PHI. Covered entities should review, and likely modify, their privacy and security policies and also their agreements with business associates. Covered entities must also ensure that they (and their business associates) have effective procedures to limit the amount of PHI they use and disclose, and they should review how changes to the marketing, fundraising, disclosure accounting, and restriction request rules affect their operations.

Business associates should similarly examine their operations to ensure they comply with the applicable HIPAA provisions, and PHR service providers would be wise to review their current procedures and start any necessary revisions.

UNDERSTANDING THE STIMULUS PACKAGE

Page 4

Most important, it is key that all entities ensure that they (and their business associates) have well-documented and effective PHI handling procedures in place. The PHI handling program must include effective employee training, effective procedures to limit the amount of PHI which is used and disclosed, and effective data security procedures. In addition to being a best practice for avoiding mishandling of PHI, a well-conducted and well-documented program will be helpful in the event a breach prompts an investigation by the HHS, FTC, or state attorneys general.

Furthermore, within months, all will be required to institute breach notification procedures unless they secure data according to certain protocols to be identified by HHS in April 2009. Entities would be wise to incorporate such protocols into their PHI handling procedures in order to avoid the breach notification requirements, and even more important, to avoid data breaches.

If you have any questions regarding these new requirements, please contact Susan Gindin at 303-256-7046 or sgindin@ir-law.com. Susan has been practicing in the area of data privacy law for over thirteen years and has been providing HIPAA guidance since 2002.