AIS: Major New HIPAA Requirements: How to Comply With Strong Privacy and Security Measures Signed by President Obama

President Obama signed the American Recovery and Reinvestment Act (ARRA) of 2009 into law (Pub. L. 111-5) on February 17, 2009. Its primary purpose is to stimulate the economy; however, it also contains many Health Insurance Portability and Accountability Act (HIPAA) provisions that affect the privacy and security of health information. On Wednesday, March 11, Atlantic Information Systems, Inc. (AIS) hosted an audio-conference presented by Reece Hirsch, Esq. entitled "ARRA 2009 and the HITECH Act: The Next Phase of HIPAA Regulation and Enforcement Arrives". The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is incorporated into the umbrella ARRA. Throughout the audio-conference, Mr. Hirsch highlighted many specific measures that organizations need to comply with in the future and steps that can be made now to ensure compliance with these new HIPAA-related requirements. This brief will summarize and address many of the key provisions discussed in the audio-conference.

Breach Notification

A major provision of the HITECH Act involves the imposition of a security breach notification requirement for unauthorized breaches of Protected Health Information (PHI). Covered entities must notify individuals whose PHI, in electronic or paper form, has been, or is reasonably believed to have been breached. A breach under ARRA is defined as unauthorized access of PHI which compromises security or privacy except when the information would not reasonably have been able to be retained by the unauthorized person. Mr. Hirsch explained the meaning of the exception through a situation where a laptop containing PHI is stolen but immediately recovered giving the thief no real opportunity to access the protected information.

A real-life example of a breach came from a caller in the Question and Answer Section of the audio-conference. An individual authorized to view PHI in the medical records section of a hospital accessed the health records of a spouse to gather information for a divorce proceeding. This would be a breach and require notification. A breach, however, does not involve the unintentional access by an authorized individual if it was made in good faith within scope of employment and was not further accessed or disclosed. If the employee inadvertently accessed his spouse's PHI without any intent to gain information in a divorce proceeding and the PHI was not further accessed or disclosed, this would not have constituted a breach.

ARRA gives business associates new responsibilities and obligations in relation to breach notification. Business associates are now required to notify the covered entity of any breach. While they are not required to notify the individuals whose PHI was breached, they may fulfill their obligations under ARRA by notifying the covered entity of the breach. The covered entity would be bound to notify the individual under these new provisions.

While current HIPAA rules do not require notification to individuals, the ARRA contains several measures that describe the method and timing of breach notifications. All breach notifications under the new ARRA provision must be made within 60 days of discovery and without unreasonable delay. Procedures for carrying out notifications are described in the statute. Notice to individuals whose information has been breached needs to be made in writing and sent by written notice via first class mail or via email, if preferred by the individual. Large scale breaches of more than 500 persons require the notification of the United States Department of Health and Human Services, as well as the dissemination of the breach through "prominent media outlets." The Department of Health and Human Services will also post the information on its agency website. Further guidance on the breach notification provision is to be provided through interim final regulations within 180 days from date of enactment of the ARRA. The breach notification requirement will then be in effect for breaches discovered on or after 30 days from this interim rule publication.

The ARRA also places notification requirements on entities and vendors that maintain personal health records. These entities must notify the individual whose information was breached as well as the Federal Trade Commission based on a claim of unfair and deceptive trade practices.

Business associates

Provisions of the HIPAA Security and Privacy Rules are now directly applicable to business associates due to ARRA enactment. Business associate agreements had been the main mechanism for the description of the privacy and security requirements put on business associates under HIPAA. These agreements will no longer be the primary authority describing the security obligations of business associates. ARRA requires business associates to directly comply with the administrative, physical, and technical safeguards of the HIPAA Security Rule and develop policies and procedures to address security concerns that were only required of covered entities until this point. As an example of their heightened responsibility, violations of the Security rule will subject the business associate to the same civil and criminal penalties associated with a HIPAA covered entity. HHS will publish annual guidance to assist business associates in implementing their new obligations under ARRA. ARRA also alters the business associate responsibility under the HIPAA Privacy Rule; however, much of its obligations are still to be carried out under the contractual agreement. ARRA directs business associates to take responsibility for its use and disclosure of protected information. Business associates will be subject to HIPAA's civil and criminal penalties for violations of the Privacy Rule.

The new act also expands the definition of Business Associate by including entities that routinely access and transmit PHI in providing services for covered entities. Examples enumerated in the statute include Health Information Exchange Organizations, Regional Health Information Organizations, an e-prescribing gateways, or third-party vendors of Personal Health Records.

Limitations on Use and Disclosure of PHI

The ARRA offers new measures regarding marketing and fundraising activities of covered entities. Marketing communications that were considered health care operations under HIPAA will be more limited in scope. For example, the communication by a covered entity for use and purchase of a product or service will no longer be permitted, if that communication described a product in the covered entity plan benefits or is used for treatment purposes. These disclosures are no longer deemed health care operations if the covered entity received direct or indirect remuneration. Exceptions would include instances where: (a) the communication pertains to a current prescription medication taken by the individual and the remuneration is reasonable; (b) the communication by the covered entity is based on a valid HIPAA authorization; or (c) the business associate communication is within the terms of the written business associate agreement. Fund-raising communications are still considered health care operations and must provide an individual an option to opt-out of receiving such communications. An individual's decision to opt-out of receiving further fund-raising communications will be treated as a revocation of authorization under HIPAA.

Under the HIPAA Privacy Rule, the use and disclosure of PHI by a covered entity must be the "minimum necessary" amount to reasonably accomplish the underlying purpose of the disclosure. ARRA requires HHS to issue guidelines on the definition of "minimum necessary" within 18 months after enactment. Until these guidelines are released, ARRA directs that the use and disclosure of protected information be accomplished using a limited data set, if practicable.

The sale of electronic health records or PHI by a covered entity or business associate is prohibited under ARRA. Covered entities and business associates cannot receive direct or indirect remuneration, unless the purpose of the sale is for: (a) public health activities, as defined by the Privacy Rule; (b) research purposes subject to limitations on the remuneration; (c) treatment, unless HHS determines otherwise; (d) transfers in connection with the sale or merger of a Covered Entity; (e) remuneration paid by the Covered Entity to a Business Associate for its services regarding the exchange of protected health information; or (f) providing an individual with a copy of the individual's protected health information.

Individual Rights

The ARRA also describes the rights of individuals and obligations for covered entities associated with the protection of information in Electronic Health Records. Individuals now have a right to receive an accounting of their PHI disclosures. Under the HIPAA Privacy Rule, covered entities did not need to account for each use and disclosure of protected health information for treatment, payment and health care operations. Now, covered entities that use electronic health records must account for such disclosures. HHS will issue regulations regarding the information to be kept by the electronic health record for approved purposes, such as for treatment, payment, or health operations.

These accounting provisions become effective at different dates depending upon the date the covered entity acquired electronic health records. For a covered entity that utilized electronic health records as

of Jan. 1, 2009, this requirement applies to disclosures made on or after Jan. 14, 2014. For covered entities that obtained electronic health records after January 1, 2009, the provision will be effective for disclosures on January 11, 2009, or the date the entity obtains the electronic health record, whichever is later.

Increased penalties for noncompliance

The ARRA emphasizes the increased civil and criminal penalties associated with the violation of the new privacy and security provisions. Formal investigations by HHS are required if a preliminary investigation into the facts shows that the violations of the ARRA provisions were a result of willful neglect. Further, ARRA authorizes state Attorneys General to bring an action in federal court on behalf of a state resident when the resident's interests have been threatened or adversely affected due to a HIPAA violation. Finally, ARRA increases the severity of Civil Monetary Penalties associated with the violation of these provisions. The penalty increases dramatically depending on the level of neglect associated with the violation. These monetary penalties went in effect upon enactment.

Conclusion

The ARRA contains many provisions that affect the privacy and security of health related information. Increased responsibilities for covered entities and business associates, as well as increased penalties of noncompliance, highlight the major changes in HIPAA-related regulations. The definition of business associates was expanded to include new types of entities. The effect of all the changes made by the ARRA will not be fully known until all of the regulations are released, but it suffices to say that these changes will have a significant impact on the health information technology field in the future.