

American Recovery and Reinvestment Act of 2009 Updates to HIPAA

Overview

On February 17, 2009, President Barack Obama signed the *American Recovery and Reinvestment Act of 2009* (ARRA). ARRA is an economic stimulus bill that allocates \$787 billion in funding for science, engineering research and infrastructure, education, social sciences, and the arts. Title XIII, Division A of ARRA comprises the provisions of the *Health Information Technology for Economic and Clinical Health Act* (HITECH). HITECH represents a historic investment in health information technology to improve the quality of health care delivery and patient care. The programs funded under HITECH are intended to work in combination to provide the necessary technical assistance for providers to become meaningful users of EHRs, coordinate the state's efforts with regard to the electronic exchange of health information, and provide the needed training and education to increase the health IT workforce. These changes create new requirements, enforcement provisions, and penalties for covered entities, Business Associates, vendors, and others in how protected health information (PHI) is stored and used. The following lists the major privacy and security changes as a result of the ARRA:



ARRA Changes to HIPAA

- Business Associates will be subject to the same HIPAA security provisions as covered entities for implementing administrative, physical, and technical safeguards on PHI. They are also subject to civil and criminal penalties for violation of these Business Associate requirements.
- Federal law now requires consumer notification of data breaches involving “unsecured” PHI or information not secured through the use of technology or methodology specified in guidance by the Department of Health and Human Services (HHS). Both covered entities and Business Associates must comply.
- The Business Associate of a covered entity that obtains or creates PHI shall use and disclose this information in compliance with the terms of the signed Business Associate agreement or arrangement.
- The designation of a privacy advisor in each region by the Secretary of HHS and the establishment of an educational initiative by the HHS Office for Civil Rights to provide education on health information privacy.
- Vendors of PHI and their service providers are subject to the same security breach notification requirements regarding PHI as for Business Associates to covered entities and for covered entities to individuals in reporting a breach of unsecured PHI to the consumer.
- Restrictions are in place on the remuneration for “sale” of electronic health records (EHRs) or PHI unless the client has signed a written authorization in compliance with HIPAA.
- Individuals may require covered entities not to disclose certain self-pay services to health plans.

ARRA Changes to HIPAA (cont.)

- Covered entities must use, disclose, or request a limited data set, or the minimum necessary of PHI to accomplish the intended purpose of such use, disclosure, or request.
- Upon request, covered entities using EHRs are required to provide an individual with an accounting of disclosures of PHI for treatment, payment, and health care operations.
- Upon request, covered entities using EHRs must also provide an individual's information in electronic form and transmit it to third parties.
- A Business Associate or covered entity must sign a Business Associate agreement for the release of PHI to health information exchanges.
- The HIPAA health care operations exception on use of PHI for "marketing" communications is narrowed significantly, if direct or indirect remuneration is received.
- Individuals have the right to opt-out from receipt of a covered entity's fund raising communications.
- A violation in obtaining or disclosing individually identifiable health information is criminal under the Social Security Act was clarified.

The Act provides for "improved enforcement" and the HHS Secretary may enforce and impose set penalties for HIPAA violations due to "willful neglect."

Implementation

The passage of the ARRA directed the Secretary of HHS to amend the HIPAA Privacy and Security rules to implement these legislative changes. The changes to the privacy and security portions of the ARRA are currently in effect. Upon request, covered entities using EHRs are required to provide an individual with an accounting of disclosures of PHI.

