

American Recovery and Reinvestment Act Changes to the Health Information Privacy and Security Rules



American Recovery and Reinvestment Act Changes to the Health Information Privacy and Security Rules

The recently passed American Recovery and Reinvestment Act ("ARRA") also makes extensive changes to the privacy and security regulations of the Health Insurance Portability and Accountability Act ("HIPAA"). The good news – immediate action is not required. The bad news – business associate agreements, policies and procedures, notices of privacy practices and training materials must be updated once additional guidance and/or effective dates arrive.

Highlights

Business Associates

- Effective February 17, 2010, business associates will be directly subject to the HIPAA privacy and security rule. Currently, HIPAA only applies directly to covered entities, and a business associate is only indirectly regulated by HIPAA through the business associate agreement established with the covered entity.
- Business associates will also be subject to civil and criminal penalties and enforcement proceedings for violations of the HIPAA privacy and security regulations.
- Effective February 17, 2010, an organization that provides data transmission services to a covered entity (and/or another business associate) will be deemed to be a business associate.

Notice of Breach

- Effective 30 days after guidance is issued, covered entities (and presumably business associates) must notify any individual affected by a breach of "unsecured" PHI and keep a log of such breaches to submit to Health and Human Services ("HHS") on an annual basis. The ARRA sets forth the content requirements for the notice as well as when the notice must be provided to affected individuals. Guidance regarding "unsecured" PHI is required to be issued by April 18, 2009, while interim final regulations regarding the duty to notify must be issued by August 16, 2009.

Individual Rights

- If a covered entity discloses PHI to carry out treatment, payment or health care operations and such disclosures are made through an electronic health record, individuals may request an accounting of such disclosures. The ARRA defines an electronic health record as an electronic record of health-related information on an individual that is created, gathered, managed or consulted by authorized health care clinicians and staff. With regard to electronic health records held by a covered entity as of January 1, 2009, this new accounting requirement will apply to disclosures on or after January 1, 2014. With regard to electronic health records acquired after January 1, 2009, this requirement will apply to disclosures on or after January 1, 2011.
- If a covered entity uses or maintains electronic health records that contain PHI, effective February 17, 2010, an individual may request a copy of his or her record in electronic format or may direct the covered entity to send a copy to another entity or person. The covered entity may charge for labor costs associated with responding to the request.
- If an individual pays his or her health care treatment or services out-of-pocket in full, he or she can prohibit the health care providers from disclosing PHI to his or her health plan.

Limited Data Sets; Minimum Necessary

- The ARRA requires covered entities to limit their use and disclosure of PHI to limited data sets if possible. A limited data set is de-identified information except the information can have dates more specific than year and locations down to zip code.
- Additional guidance on the “minimum necessary” standard should to be issued no later than August 17, 2010.

Enforcement; Penalties

- The ARRA requires HHS to audit covered entities regarding HIPAA privacy and security compliance and to formally investigate a covered entity upon receipt of a complaint.
- The ARRA amends HIPAA to increase the civil and criminal penalties for HIPAA violations based on different levels of intent. The ARRA also clarifies that, for purposes of the criminal provisions, individuals (who are not themselves covered entities) may be convicted of criminal violations of HIPAA. The increased civil penalty amounts apply to violations after February 17, 2009.
- The enforcement provisions are expanded such that state Attorneys General have the power to bring civil actions in federal court against any person whose HIPAA violations pose a threat to or harm one or more residents of the state.

Regulations related to these enforcement provisions are required to be issued by August 17, 2010. In addition, HHS is required to issue regulations within the next three years that would provide individuals who have been affected by a HIPAA violation the right to receive a percentage of any civil monetary penalty or monetary settlement collected.