



ARRA Not Just for COBRA Subsidy: New HIPAA Provisions

While most employers and insurance carriers are scurrying to understand and comply with the new COBRA subsidy rights, some of the other provisions of the ARRA haven't received much attention. The ARRA provisions make significant changes to HIPAA's privacy and security requirements, specifically expanding and enhancing privacy and security safeguards for certain individually identifiable health information.

More Entities Covered: Business Associates

Under HIPAA, individuals and entities are generally treated as "business associates" when they provide services to covered entities (i.e., health care providers, plans, and clearinghouses). In the past, business associates were not directly subject to the privacy and security regulations under HIPAA, but rather indirectly through the service agreements with the covered entities. Under ARRA, beginning 12 months from ARRA enactment (Feb. 17, 2009), HIPAA privacy and security laws apply directed to business associates.

Breach Notification

Previously, covered entities were obligated to mitigate harm caused by unauthorized disclosures of protected health information, but not required to give notice to the individuals whose information was inappropriately disclosed. Going forward, covered entities and business associates will be required to notify individuals when security breaches occur with respect to "unsecured" information. Unsecured information means information not protected through technology or methods designated by the federal government.

A breach requiring notification does not occur where the unauthorized person who receives a disclosure of protected health information would not reasonably be able to retain the information. Unless delay permitted for law enforcement purposes, notification may not be provided later than 60 days after discovery of the breach. If the breach involves 500 or more individuals, notice to the federal Department of Health and Human Services. Breaches involving 10 or more individuals for whom there is insufficient or out-of-date contact information requires conspicuous posting on covered entity's website or with major media outlet.



The ARRA directs the Department of Health and Human Services (HHS) to promulgate regulations within 180 days of the date of enactment to carry out this new notification requirement.

Stepped Up Enforcement

Effective upon enactment, State Attorneys General may bring civil actions in federal court to obtain injunctive relief or damages on behalf of state residents who have been, or are threatened or adversely affected by violations of HIPAA. Previously, HIPAA did not permit individuals to obtain monetary damages for HIPAA violations and enforcement was handled at the federal level. The financial penalties for violations of HIPAA have also been increased, and a percentage of the civil penalties collected will be distributed to individuals harmed by the violations.

Since April 14, 2003, the original effective date of the HIPAA privacy regulations, civil penalties have been infrequently assessed. The ARRA appears to look to change that. In addition to the increase in penalties, beginning two years after the date of enactment of ARRA penalties will be required in cases of willful neglect, and beginning three years of enactment, a method will be in place to share civil penalties with the individuals harmed.

Timing Considerations

Covered entities and business associates will need to take measures to comply with the new requirements. Covered entities may need to modify their business associate agreements. Business associates will be subject to statutory requirements as well as contractual requirements. Effective dates vary. Most of the new security rules will take effect later this year (30 days after HHS publishes related regulations). Most of the new privacy rules will take effect one year after ARRA is signed into law. The new penalty and enforcement rules are effective immediately.