

KEEPING CURRENT . . . on COBRA & HIPAA[®]

The *AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009* (ARRA) was signed by the President on February 17, 2009. This issue is one of several *ARRA Special Editions* I will be sending as additional information is received.

Correction to COBRA NOTICES Article...

(March 23, 2009 Edition)

The General Notice (Abbreviated version) would ***NOT be used as an attachment to the Election Notice...*** it is used only for individuals who experienced a qualifying event during on or after September 1, 2008, have already elected COBRA coverage, and still have it.

ARRA and HIPAA AMENDMENTS

As I reported in previous editions, ARRA amends certain HIPAA Privacy and Security provisions. Most of these provisions are not effective until February 17, 2010, but it may take a year to revise policies, procedures and HIPAA documents to comply with these new and expanded requirements.

- Specific Notification Procedures for Breach of "Unsecured" PHI (effective 30 days after interim final regulations published) - ARRA directs HHS within 60 days of ARRA's enactment to identify technologies to ensure that information is secure, and to publish interim final regulations within 180 days of ARRA enactment. CEs that use the protocols that HHS specifies can avoid the extensive breach notification requirements: CEs must notify every individual potentially affected by a breach "promptly". For breaches involving less than 500 individuals, CEs must keep a log and submit annually to HHS. For breaches involving 500 individuals or more, CE must also notify HHS and prominent media outlets serving the area, and HHS will post the breach on their website.
- Business Associates (BA) are now re-characterized as Covered Entities (CE) and explicitly required to comply with the Privacy Rule and all portions of the Security Rule, including administrative, physical and technical safeguards. Previously a BA was only contractually liable to a CE for any breach of the BA agreement; they are now *directly liable for the same fines and penalties as CEs*. CEs may need to amend the BA language to ensure the new requirements are included; BAs will need to ensure they are in compliance with all HIPAA requirements.
- The definition of a BA has been expanded to include any entity that provides data transmission of PHI to a CE or its BAs and requires routine access to PHI.
- Restrictions on PHI Disclosures - Current HIPAA provisions allow an individual to request that a CE limit certain disclosures of PHIO, but a CE is not required to agree to the request. Under ARRA, if the individual has paid in full out of pocket for the treatment, the CE must agree to the request. Accounting of PHI Disclosures (effective Jan. 1, 2011) - HIPAA required a CE to provide an individual with an accounting of any disclosures made for up to six years except for Treatment, Payment or Health Care Operations (TPO). Under ARRA, CEs that use or maintain Electronic Health Records (EHR) will be required to provide individuals with an accounting of PHI disclosures made to carry out TPO for up to 3 years.
- Enhanced Enforcement (effective for violations occurring after 02/19/09) - ARRA includes a new four-tiered civil penalty structure with fines up to \$50,000 per violation and an annual cap of \$1,500,000 and authorizes State Attorney Generals' to bring civil actions for monetary damages. ARRA also clarifies that criminal penalties apply to employees and individuals, not just to the CEs. In addition, ARRA requires HHS to periodically audit CEs and BAs to ensure compliance with HIPAA (rather than the current complaint-driven process).

For more information on these topics, contact:

Marlene H. Mehringer Bowen, LUTCF, RHU

(812) 449-9782

marlene@mehringerasociates.com

