Employer Compliance Alert

COORDINATED BENEFITS COMPANY, LLC
www.cbcco.com

DUST OFF YOUR HIPAA HATS: Major Changes To HIPAA Privacy And Security Rules Are On The Way

After a few years of relative calm after the "HIPAA storm," it appears that clouds are on the horizon for employers, plan administrators, and business associates. In addition to the new COBRA subsidy requirements (as discussed in our recent Compliance Alert), another of the items included in the recent economic stimulus package (formally known as the American Recovery and Reinvestment Act or "ARRA") was a significant expansion of the HIPAA privacy and security rules. While Congress has given covered entities and business associates a bit more time than it gave employers to comply with the new COBRA rules, they should still act quickly to review and digest the new HIPAA requirements.

Business Associates

The most significant change in the new rules is the extension of certain HIPAA provisions to "business associates." Previously, the HIPAA rules made a clear distinction between "covered entities" (to which all of the HIPAA privacy and security rules apply) and "business associates" (which were not directly covered by the HIPAA rules, but with whom covered entities were required to obtain business associate agreements). Under ARRA, certain HIPAA security provisions now apply directly to business associates to the same extent that such provisions apply to covered entities, including the potential application of civil and criminal penalties for violations of HIPAA.

This is a major sea change for business associates such as third-party administrators and other vendors who previously thought that their sole legal obligation was to comply with the terms of the business associate agreement. These changes will require a major effort by business associates, including appointing a security officer, developing written security policies and procedures, and training their workforce on how to protect electronic protected health information ("PHI").

Notification in the Case of Breach

Covered entities that hold, use or disclose "unsecured" PHI must now notify affected individuals in the event of a breach of the information. Under existing law, covered entities merely had an obligation to mitigate any breach, but

not necessarily to notify the affected individual. The term "unsecured" is not yet defined but will ultimately be determined under guidance to be issued by the Secretary of Health and Human Services. Such guidance is expected to be issued within 60 days of ARRA's enactment (or by mid-April).

Furthermore, business associates, who already had an obligation to notify covered entities of an unauthorized disclosure of PHI in their possession, must now specifically include in their notice the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. In both cases, notice must be provided without unreasonable delay and in no event later than 60 days after the discovery of the breach. Generally, the notice must be provided to each individual, in writing, by first-class mail. However, if the breach involves the unsecured PHI of more than 500 individuals in a particular state or jurisdiction, notice must also be provided to prominent media outlets serving that state or jurisdiction.

Requests for Restrictions

Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the disclosure of their PHI. Previously, covered entities were not necessarily required to agree to the requested restriction. Now, however, a covered entity must comply with the requested restriction if the disclosure is to a health plan for a payment or health care operations purpose (but not if it is for treatment purposes) and if the PHI pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket in full. For example, it appears a covered dependent child can now specifically request that a health plan not disclose to the child's parent any PHI in its possession relating to health care services for which the child has paid in full.

Accounting of Disclosures for Use of Electronic Health Records

ARRA creates a new term, "electronic health record" (or "EHR"), which is defined as an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. Under existing law, an individual has the right to an accounting of certain disclosures, but such right does not extend to disclosures that are otherwise permissible for treatment, payment, or health care operations purposes. To the extent that a covered entity makes such disclosures in connection with its use or maintenance of an electronic health record, such disclosure must now be accounted for even if it is for treatment, payment, or health care operations purposes. In contrast to the regular right to an accounting for up to six years, an individual has the right to request an accounting of EHR disclosures for up to only three years. While these rules appear to be targeted primarily at health care providers, it is not clear whether they will continue to apply when an EHR is transferred to a health plan, employer, or business associate.

Increase in Civil Monetary Penalties

The civil monetary penalties for a violation of the HIPAA Privacy Rule or Security Rule have been significantly increased. In general, the penalty for violations due to reasonable cause and not to willful neglect has increased

ten times, from $100 per violation to $1,000 per violation. Violations that are found to be due to willful neglect (even if corrected) are subject to a penalty of $10,000 per violation. Additionally, although there is still no individual private cause of action under HIPAA, state attorneys general can now bring an enforcement action and obtain damages (including attorneys' fees) on behalf of residents of that state.

Effective Dates

The general effective date for most of these changes, including the changes to the business associate rules, is one year after the date of ARRA's enactment, or February 17, 2010. However, the increase in civil monetary penalties is effective immediately, and the duty to notify individuals of security breaches will be effective 30 days after regulations are issued by the Department of Health and Human Services.

Julia Vander Weele
Partner, Spencer Fane Britt & Browne LLP

COORDINATED BENEFITS COMPANY, LLC
923 North Plum Grove Road, Suite C • Schaumburg, IL 60173-5152
Phone: 847.605.8560 • Fax: 847.605.8566 • Website: www.cbcco.com