New Health Information Privacy and Security Provisions in the American Recovery and Reinvestment Act of 2009

February 25, 2009

SECURITY & PRIVACY ALERT - FEBRUARY 25, 2009

written by Colin J. Zick

Somewhat lost in the American Recovery and Reinvestment Act of 2009 ("ARRA"), among the hundreds of pages describing billions in stimulus spending and tax relief, are significant new health information privacy and security provisions. These provisions have the potential to impact every "covered entity" under HIPAA, including hospitals, physicians and health plans, as well as "business associates" who were not previously covered by HIPAA. Among these new provisions are:

- **Extension of certain HIPAA security rules to "business associates"**

  In particular, HIPAA Security provisions regarding Administrative Safeguards (45 C.F.R. § 164.308), Physical Safeguards (45 C.F.R. § 164.310), Technical Safeguards (45 C.F.R. § 164.312) and Policies & Procedures and Documentation Requirements (45 C.F.R. § 164.316) will soon apply directly to HIPAA business associates "in the same manner that such sections apply to the covered entity." See ARRA Sec. 13401(a).

  Civil and criminal penalties for improper disclosure of health information also will apply to "business associates", exposing them to the same liability as HIPAA "covered entities". These penalties top out at 10 years in jail and fines of $250,000 for improper use of protected health information. See ARRA Sec. 13401(b).

- **New federal security breach notification law**

  A covered entity that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information" will be required to respond to any data breach. These provisions have the potential to be quite burdensome: upon discovery of a breach, the covered entity is required to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach." (Emphasis added.) This notice will have to be provided within 60 days of the breach. See ARRA Sec. 13402(b). Business associates will be required to provide similar notice to their covered entities in the event of a breach. When 500 or more individuals are involved, the covered entity will be required to notify major media outlets and HHS. Precisely how these provisions will interact with state data breach laws has yet to be determined.

- **Extending the "minimum necessary" standard**

Previously unrestricted uses and disclosures, such as to individuals or for treatment, payment or health care operations will be subjected to the "minimum necessary" limits on disclosure. HHS is required to issue regulations to define just what "minimum necessary" means. See ARRA Sec. 13405(b).

- **Tighter rules on when PHI can be used for marketing purposes**

  Under ARRA Sec. 13405(d), a specific patient release will be needed before protected health information can be sold: "a covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any protected health information of an individual unless the covered entity obtained from the individual . . . . a valid authorization that includes, in accordance with such section, a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual."

- **New rules for fundraising communications**

  Marketing communications will be clearly carved out of HIPAA's definition of "health care operations": "[a] communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation . . . ." See ARRA Sec. 13506(a).

- **Stepped up enforcement efforts by HHS**

  The Secretary of the Department of Health and Human Services is directed to conduct "periodic audits to ensure that covered entities and business associates". See ARRA Sec. 13411. It is unclear from the text of ARRA how many of these audits will be conducted, or what subjects will be audited.

Most of these provisions are set to take effect a year from the enactment of ARRA, on February 17, 2010. In the interim, we expect HHS to be active clarifying how these new provisions will be applied. If you would like a copy of these new provisions, go to our blog, www.securityprivacyandthelaw.com. If you have questions about these provisions and how they apply to you or your company, or wish to review your existing HIPAA compliance in light of these changes, please contact Colin Zick at 617 832 1275.