Stimulus Circus: Taming the HIPAAs and COBRAs – Practical Steps to Dealing with Regulatory Change

By Shannon Hartsfield Salimone and Dana Gryniuk

The stimulus bill passed in February 2009, also known as the American Recovery and Reinvestment Act of 2009 (the "Act"), contained many provisions dealing with health care. Some of those changes deal with health privacy and security in particular. Health care providers and businesses subject to the Health Insurance Portability and Accountability Act ("HIPAA") may not be thrilled to learn that the Act contains new HIPAA compliance obligations; however many of these obligations will be important for further protecting and documenting protected health information ("PHI") in this new electronic age.

There are regulations anticipated that, presumably, will shed more light on these new requirements under the Act. Many health care providers, also known as covered entities ("CEs") under HIPAA, and the third parties who receive PHI from those entities or on their behalf, also known as business associates ("BAs"), cannot sit back and wait for those regulations. There are things that CEs, like hospitals, doctors, clinics, health insurance companies, other health care entities, and their BAs need to know now about the new Act.

For example, there are some new defined terms, such as “electronic health record" and "personal health record." Exactly what levels of security or protection apply to an individual’s PHI under the Act depend on how that information is defined. There are new HIPAA privacy rules that apply to a CE and a BA and those privacy requirements must also be included in the BA agreement with the CE. Also, under the Act, if a BA has knowledge that its CE is breaching the BA agreement, the BA has the same obligations as a CE previously did under the old laws, like taking steps to end the violation or cure the breach, or terminating the BA agreement and relationship.

In terms of security, current HIPAA security standards that applied to CEs now apply to BAs, including administrative safeguards, physical safeguards and technical safeguards. Those safeguards have to be incorporated into the BA agreement. Under the new provisions, HIPAA civil and criminal penalties now also apply to BAs in same manner as they did to the CEs. Moreover, individuals (not just their employer CEs and BAs) can be civilly and criminally penalized for violations. The new law has also increased penalty tiers for the different levels of violations. Other interesting changes related to penalties and enforcement include the possibility of harmed individuals being able to receive a percentage of the civil money penalties collected from a violation of their rights under HIPAA. Additionally, the attorneys general in the various states will be given HIPAA enforcement authority.

The Act also contains new requirements for privacy and security breaches. Under the old HIPAA Privacy Rule and Security Rule, a CE had to try to mitigate a PHI breach, or minimize any harm. Sometimes, the CE might determine that notice to patients was unnecessary to mitigate a breach. Now, notice to patients is required regardless of whether the CE feels it is necessary. All notifications must be made without "unreasonable delay" and in no case later than 60 calendar days after discovery.

There are also new restrictions on disclosures of PHI to health plans if an individual requests it. Other changes include new marketing rules, changes to disclosures using a limited data set and the minimum necessary standard, tracking for EHRs, prohibitions on receiving remuneration in exchange for PHI, and rules for vendors of personal health records. Much of the new provisions take effect in February of 2010, however, the increased HIPAA penalties are effective right now and the breach notification requirements come into play for breaches 30 days or more after the development of an implementing rule, which is required 180 days from when the Act passed, or in August of 2009.

These HIPAA changes present a golden opportunity to revisit data privacy and security. Some entities subject to HIPAA may not have dusted off their compliance plans in quite a while. Certain policies may be outdated. There is no time like the present to give employees a reminder of their current and new obligations, update policies and procedures, implement required internal systems or technology, and amend BA agreements to ensure compliance with the Act.

Shannon Hartsfield Salimone is a partner in Holland & Knight’s Tallahassee office whose practice focuses on health care regulation and data privacy. For 14 years, she has advised long term care companies, physicians, health plans, hospitals, employers, and other entities on questions related to information privacy and security. Dana Gryniuk is an associate in Holland & Knight’s Miami office. Her practice focuses on corporate law and healthcare regulatory and licensing matters, including Medicare and Medicaid, for various health related facilities and providers.