In Post-HITECH Era, HIPAA Ignorance Could Be Costly
By: Amy K. Fehn, Wachler & Associates, P.C.

Individuals or entities that use or have access to patient information in the course of providing services to health care providers should be prepared for heightened scrutiny in the upcoming year. While entities meeting the definition of a "business associate" have always been required contractually to comply with the Health Insurance Portability and Accountability Act (HIPAA) requirements, they will now have direct liability. Further, a proposed rule that is expected to be finalized in late 2010 or late 2011 will likely expand the definition of business associate even further.

In July 2010, CMS issued a proposed rule[1] implementing modifications to HIPAA[2] as a result of the HITECH Act.[3] A final rule is expected to be issued in late 2010 or early 2011. However, business associates of covered entities should not delay compliance efforts, as they already have direct liability for HIPAA breaches and increased penalties as a result of the HITECH Act, even without a final rule.

In general, and subject to certain additions and exceptions, a "business associate" pursuant to the HIPAA regulations is a person or entity that provides services to a "covered entity", such as a health care provider, which involve the use of "protected health information." Examples of business associates include billing companies, collection agencies, shredding services, and law firms that require the use of "protected health information" to provide services.

Prior to the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH), business associates were contractually liable to the covered entities for which they provided services. They were not, however, directly liable to the government for a HIPAA violation.

Pursuant to the HITECH Act, the government can now impose penalties directly on business associates who violate the HIPAA requirements. The proposed rule, if finalized, goes one step further and allows the government to imposed penalties directly on subcontractors of business associates, as well as the subcontractors' subcontractors (and any other "downstream" subcontractors). Although it is the covered entity's responsibility to have contracts in place with business associates and the business associates' responsibility to have contracts in place with subcontractors, the proposed rule clarifies that the government can impose liability on the business associates or subcontractors even if such contracts are not in place.[4] Thus, business associates and subcontractors are responsible for determining whether they are bound by the HIPAA regulations, even if they are not asked to enter into a contract.

---

[1] 75 Fed. Reg. 40868 (July 14, 2010).
[2] The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191.
[3] The Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 115).
[4] 75 Fed. Reg. 40888 (July 14, 2010).

Like covered entities, business associates and their subcontractors are required to make uses and disclosures only as permitted by HIPAA and are required to have HIPAA Privacy policies and procedures. Business Associates are also required to comply with the HIPAA Security Rule, including administrative, physical and technical safeguards. Business Associates also are responsible for complying with the recently enacted breach notification provisions.

Pursuant to the HITECH Act and the proposed rule, business associates are also required to apply the "minimum necessary" rule when making requests for information to provide services to a covered entity.[5] If a business associate requests more than the "minimum necessary" information from the covered entity, the business associate will be in violation of the HIPAA Privacy Rule.

In addition, as discussed above, business associates are required to enter into agreements with any subcontractors who receive protected health information in the course of providing services to the business associate.[6] Failure to have these contracts in place is not only a violation of HIPAA, but also subjects the business associate to liability for any of its subcontractors' violations.[7] A business associate can also have liability for a subcontractor's violations to the extent that the subcontractor is considered to be an "agent" of the business associate pursuant to the federal common law of agency.[8] Business associates are also responsible for subcontractors' violations to the extent that the business associate knows of a pattern of noncompliance by the subcontractor and does not take reasonable steps to cure the breach.

Penalties for noncompliance are the same for business associates (and their subcontractors) as those imposed on covered entities and can be significant. The HITECH Act established four tiers of penalties based upon the level of culpability. The lowest level, with a minimum penalty of $100 per violation will be applied in situations where the business associate "did not know, and by exercising reasonable diligence would not have known" of the violation. The second tier of penalties, with a minimum of $1,000 per violation, applies to violations for "reasonable cause" which do not rise to the level of "willful neglect". "Reasonable cause" is defined in the proposed rule as a situation where the business associate knew or "should have known by the exercise of reasonable diligence" that a violation occurred. The third tier penalties, with a $10,000 minimum, are applied to violations attributed to "willful neglect", which is further defined as "the conscious, intentional failure or reckless indifference to the obligation to comply" with the HIPAA provision violated. The fourth tier of penalties apply to violations for "willful neglect" that are not remedied within thirty days of the date that the business associate knew or should have known of the violation, with minimum penalties of $50,000. All tiers of penalties have a maximum of $50,000 per violation and $1,500,000 aggregate for identical violations during a calendar year.[9]

---

[5] 75 Fed. Reg. 40877 (July 14, 2010).
[6] 75 Fed. Reg. 40888 (July 14, 2010).
[7] 71 Fed. Reg. 8402 (Feb. 1, 2006)
[8] 75 Fed. Reg. 40914; Proposed 45 CFR §160.402
[9] 45 CFR §160.404.

The importance of HIPAA policies and procedures for reducing liability is highlighted in the proposed rule, which provides several examples of lower level penalties being applied to situations where the entity had policies in place, but could not reasonably comply with a provision. (e.g., a covered entity had reasonable policies in place for allowing individuals' access, but could not handle an unusual volume of requests).[10] The proposed rule also provides examples of "willful neglect" scenarios where a violation occurred and a business associate or covered entity failed to have any policies and procedures in place.[11]

The proposed rule also clarifies that a business associate's ignorance of its HIPAA obligations does not excuse its violations. Specifically, the proposed rule clarifies that a business associate cannot assert an affirmative defense of "lack of knowledge" where it failed to inform itself about its compliance obligations.[12]

Thus, a business associate or subcontractor that fails to implement appropriate HIPAA policies and procedures could very well find itself facing hefty fines of $10,000 to $50,000 per violation, even for accidental disclosures. Because violations can be tallied based upon the number of individuals impacted and the number of days the violation continues, such violations could quickly rise to six digit levels.

It is important to note that business associates also continue to have contractual liability to covered entities, in addition to direct liability to the government. This contractual liability can exist even in situations where the business associate was not responsible for the HIPAA obligation but contractually accepted the responsibility on behalf of the covered entity. For example, if a business associate is required to distribute the notice of privacy practices for a covered entity, the breach would be attributed to the covered entity. However, the business associate would still be contractually liable to the covered entity.[13]

[10] 75 Fed. Reg. 40878 (July 14, 2010).
[11] 75 Fed. Reg. 40879 (July 14, 2010).
[12] 75 Fed. Reg. 40878 (July 14, 2010).
[13] 75 Fed. Reg. 40889 (July 14, 2010).