Casting a Vastly Expanded Regulatory Net: Implications of the New Definition of Business Associates under HITECH

By Amy K. Fehn, Wachler & Associates, P.C. and John R. Christiansen, Christiansen IT Law

as published in the ABA Health Law Section's Health E-Source

On July 14 the U.S. Department of Health and Human Services published a Notice of Proposed Rule Making for proposed regulations modifying the HIPAA privacy, security and enforcement rules ("NPRM").[1] Probably the most important single change to the HIPAA rules proposed in the NPRM is the expansion of Business Associate status to every entity which touches PHI, except on a "random and infrequent" basis, to perform a function or activity directly or indirectly "with respect to" a Covered Entity. This expanded status follows logically from HITECH's expansion of jurisdiction to regulate PHI privacy and security to Business Associates, but is likely to come as a shock to many previously unregulated entities.

Understanding this jurisdictional expansion requires a review of the reasons for the Business Associate concept. The Business Associate concept was created under the HIPAA regulations as a workaround for jurisdictional limitations under the HIPAA legislation. The HIPAA Administrative Simplification subtitle was not intended as privacy legislation. Rather, it was intended to require health care payors (insurance companies, health plans, etc.) and health care providers (hospitals, physicians, laboratories, etc.) to transmit and process health claims transactions electronically, in standardized formats and data sets.

---

[1] U.S. Department of Health and Human Services, ***Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule***, 75 Fed.Reg. 40868 (July 14, 2010)

Privacy was included in HIPAA only because of the assumption that the public would not trust the expanded use of electronic transactions involving personal information without privacy protections. Security was only included as a standard ancillary to the transactions standards, principally to help ensure the integrity of the transactions. Privacy was even less on point, and was provided for only in an uncodified section requiring privacy regulations if Congress failed to enact privacy legislation by August 1999. Congress of course did not enact such legislation, and DHHS had to develop privacy regulations that worked within the jurisdictional limitations of HIPAA's legislative intent.

This is why the HIPAA regulations distinguish Covered Entities and Business Associates. Covered Entities are the entities subject to HIPAA's jurisdiction because they engage in claims transactions, i.e. health care payor and providers (and certain claims processors called health care clearinghouses). Covered Entities could be directly required to comply with the Privacy and Security Rules in the protection and use of PHI, and penalized if they did not.

However, Covered Entities frequently need to use other kinds of entity, which are not subject to HIPAA jurisdiction, to perform a wide range of functions and activities involving the use of PHI. It would be impossible to require Covered Entities to conduct all such functions and activities themselves, but the PHI protections of the Privacy and Security Rules would be rendered meaningless if they were lost as soon as it was obtained by a non-Covered Entity.

The Privacy Rule (and later the Security Rule) therefore adopted the concept of the Business Associate. A Business Associate is defined as any "person" performs any function or activity on behalf of a Covered Entity involving the use or disclosure of PHI.[2] While Business Associates could not be reached by HIPAA directly, they were reached indirectly by regulations

[2] See 45 CFR § 160.103.

extended protections indirectly by requiring Covered Entities to have a specific form of contract, the Business Associate Contract, in place before allowing their Business Associates access to PHI. If the Business Associate violated the contract by doing something improper with the PHI the Covered Entity was required to take actions up to and including contract termination, and the Covered Entity (but not the Business Associate) could be penalized for failure to do so.

Of course, sometimes Business Associates also need additional parties to perform functions or activities involving PHI they have on behalf of a Covered Entity, and under the HIPAA regulations a Business Associate Contract could include a provision allowing them to do so if they "ensure that any [such] agent, including a Subcontractor" agrees to the same "conditions and restrictions" as apply to the Business Associate under its Business Associate Contract.[3] This has usually been interpreted as a much looser standard than the Business Associate Contract requirements, and practices in this area have often been fairly relaxed.

HITECH took these concepts and extended them, incorporating the regulatory definitions of Covered Entity and Business Associate. This was a crucial legislative move, because it extended regulatory jurisdiction related to PHI privacy and security to Business Associates as well as Covered Entities.

What was not apparent to most prior to the NPRM is that this extension now makes any party in a chain of relationships which performs a function or activity on behalf of a Covered Entity a Business Associate. Not only a Business Associate in a direct contractual relationship with a Covered Entity, but also that Business Associate's Subcontractor, and the Subcontractor of that Subcontractor, and so on as far as the PHI and functions flow – any entity in that chain fits the definition of a Business Associate.

---

[3] See 45 CFR § 164.504(e)(2)(ii)(D).

This application of this logic becomes clear in the revised definition of "Business Associate" and the new definition of "Subcontractor" in the NPRM. "Subcontractor" is now proposed to be defined as a "person who acts on behalf of a Business Associate, other than in the capacity of a member of the workforce of such Business Associate." The definition of Business Associate is also now proposed to be modified to add Subcontractors, even though they do not have a direct relationship to the Covered Entity. Since a Subcontractor is now defined as a Business Associate, it follows that any person which acts on behalf of such a Subcontractor/Business Associate performing a function or activity involving PHI is also a Subcontractor, and therefore a Business Associate.

The preamble to the NPRM gives the following example:

> . . . if a Business Associate, such as a third party administrator, hires a company to handle document and media shredding to securely dispose of paper and electronic protected health information, then the shredding company would be directly required to comply with the applicable requirements of the HIPAA Security Rule . . . and the Privacy Rule.[4]

And this Business Associate status is triggered by the performance of the function or activity involving PHI, whether or not the parties have a contract:

> Even though we use the term ''Subcontractor,'' which implies there is a contract in place between the parties, we note that the definition would apply to an agent or other person who acts on behalf of the Business Associate, even if the Business Associate has failed to enter into a Business Associate contract with the person.[5]

---

[4] NPRM at 40873.
[5] Id.

The only exception to this proposed rule is for Subcontractors which are "conduits," i.e., "data transmission organizations that do not require access to protected health information on a routine basis" and "do not access the information other than on a random or infrequent basis[.]"[6]

It is important for Business Associates to be aware of its "Subcontractor" relationships that require a contract between the entities, because failure to have such an agreement is not only a violation of HIPAA, but also subjects the Business Associate to liability for any of the 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 Subcontractors are the same 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

---

[6] Id.
[7] 71 Fed. Reg. 8402 (Feb. 1, 2006)
[8] 75 Fed. Reg. 40914; Proposed 45 CFR §160.402

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. 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, are subject to the highest penalties, 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]

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

[9] 45 CFR §160.404.
[10] 75 Fed. Reg. 40878 (July 14, 2010).
[11] 75 Fed. Reg. 40879 (July 14, 2010).
[12] 75 Fed. Reg. 40878 (July 14, 2010).

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]

In summary, it is important for Business Associates and Subcontractors to understand their obligations under the HITECH Act and to take these obligations seriously or risk serious financial penalties.

[13] 75 Fed. Reg. 40889 (July 14, 2010).