

New Players Involved

HITECH Privacy Rules to HIPAA

By Jeffrey A. Andrews, Attorney

The *Health Insurance Portability and Accountability Act* (HIPAA) was enacted in 1996 but the legislation was so massive and complex that the privacy provisions were not fully established for healthcare clearinghouses, health plans and healthcare providers (“covered entities”) for another seven years. The HIPAA Privacy Rule provided the first comprehensive federal protection for the confidentiality and privacy of patient records and health information.

In general, the Privacy Rule requires covered entities to inform patients about their privacy rights, adopt clear privacy procedures, designate an individual privacy officer to be responsible for the adoption and enforcement of these procedures, require employee training to ensure privacy procedure understanding, and manage patient records to ensure that protected health information (PHI) is only available to those who need to use it.

Since its inception, the HIPAA Privacy Rule has walked a thin line between enhancing patient medical record privacy without interfering with a patient’s access to quality delivery of healthcare services. A key element in ensuring the privacy of PHI was the development of the concept of a “business associate.” It was clear to the drafters of HIPAA that most covered entities do not carry out all their healthcare activities and functions alone. Assistance is required from a variety of contractors or other allied businesses. It is these first-tier assisting service entities that are the business associates. As medical records moved from paper copies locked in file cabinets to records transmitted electronically, the need for protection from unauthorized and unnecessary review and access increased dramatically.

The privacy provisions of HIPAA only applied to covered entities so business associates were called upon to provide assurances to covered entities in the form of the contractual terms of a “business associate agreement.” This agreement was designed to ensure that a business associate would use the PHI only for the purposes for which it had been engaged, that it would safeguard the PHI, and it would cooperate with the covered entity to provide individuals with access to the PHI upon request. After operating under the HIPAA Privacy Rule for nearly seven years, privacy advocates convinced Congress that additional protections and enhanced sanctions were necessary, and the HITECH provisions of the *American Recovery and Reinvestment Act* were enacted to address a number of troubling electronic health record issues.

HITECH Amendments

The Department of Health and Human Services (HSS) published proposed regulations on July 14, 2010 to implement the *Health Information Technology for Economic and Clinical Health Act* (HITECH) amendments to the HIPAA Privacy Rule. The regulations introduced the concept of subcontractors as well as the principle of “agency” to the relationship between covered entities and business associates.

These proposed regulations have not been well received within the healthcare industry. Hospital, physician, and insurance industry groups continue to lobby HHS for withdrawal or substantial modifications to the regulations. Nevertheless, as of this writing, the July 2010 HITECH proposed rules remain unchanged and in force.

Subcontractors are one tier farther down the chain of entities who receive and handle PHI. Think of a subcontractor as providing for the business associate the same services that the business associate offers the covered entity. The subcontractor concept is a major revision to HIPAA privacy standards and many more people and entities now fall under the provisions of the Privacy Rule.

HITECH not only expands the universe of people and entities subject to HIPAA (the subcontractors), but this notion of agency, as interpreted by the Office for Civil Rights, extends HIPAA statutory remedies up the chain for transgressions by lower tier entities. For example, if a business associate or subcontractor is deemed to be acting as an agent of the other, then the covered entity and/or business associate would be liable (or, at least, share the liability) if an enforcement action for a violation of the HIPAA Privacy Rule were to occur against a downstream agent acting within the scope of its authority.

The lessons to be learned from these HITECH related revisions to the HIPAA Privacy Rule are not well defined. Under current HITECH regulations, certain facts and conclusions are supported by legislation and regulations.

Covered Entities

Existing business associate agreements must be reviewed and modified in order to account for the addition of subcontractors to the privacy and liability matrix. Covered entities should require each business associate to disclose the subcontractors with whom they may be dealing.

Remember that privacy infractions by a subcontractor can now (through agency principles) push liability upstream to the covered entity. This means that all subcontractors should be thoroughly vetted by the covered entities and the business associate agreements should permit covered entities to veto the choice of subcontractors by business associates if the covered entities reasonably believe the subcontractors are a liability risk.

If your attorney is representing a covered entity, you may also want to modify the agreement with the business associate to define what constitutes an agency relationship as opposed to an independent contractor status. Although certainly not dispositive (because the agency relationship is not defined under HITECH but must rely on common law concepts), this portion of the business associate agreement could provide support for the covered entity should it argue that the business associate's transgressions may not be attributed to the covered entity.

Business Associates

Agreements between business associates and subcontractors will need to specifically identify the subcontractors' obligations to business associates (scope of the agency) in the same manner as business associates are obligated to covered entities. For example, the agreement with a subcontractor should require that if a privacy breach occurs, the subcontractor would notify the business associate within a specified time. It is also important that the agreement with the

subcontractor delineate which of the entities will notify patients, the Office of Civil Rights and the media (if applicable) in the event of a breach.

Another issue critical to any agreement with subcontractors concerns indemnification issues and costs associated with a breach. Will credit monitoring services, for example, be offered to those whose PHI has been compromised? Who will pay for these services?

Just as it was important for a covered entity to be comfortable with the reputation of subcontractors, business associates have an even greater incentive to work only with reputable subcontractors. Any agreements between business associates and subcontractors must define the agency relationship and the scope of the subcontractors' authority. In the event of a downstream privacy violation, business associates can try to avoid liability by contending that the violator was an independent contractor or that the subcontractor agent was acting outside its scope of authority.

Subcontractors

The issue of subcontractors is an area of HIPAA privacy that did not exist prior to the enactment of HITECH. Parties contracting with a business associate must now clearly understand the obligations and liabilities for an entity dealing with protected health information under the terms of the HIPAA Privacy Rule as amended by HITECH.

These subcontracting parties must be able to ascertain whether their services are likely to be characterized as those of an agent for the business associate or that of an independent contractor. Since neither HIPAA nor HITECH defines "agency," we must look to the common law for help.

The primary factor in determining whether an agency relationship exists turns on the level of control that a principal exerts over the agent. Of secondary importance is how the particular relationship appears to third parties. As a general rule, if a principal controls the results, and also the means to achieve those results, then an agency relationship has been established.

The relationship between the healthcare provider and the company hired to store medical records is an example. If the record storage company is off-site and offers these same services to other customers, including non-healthcare related clients, then you are probably looking at an independent contractor relationship.

Conclusions

Changes to the HIPAA Privacy Rule are still evolving under the HITECH amendments. Proposed regulations, many of which have been highly contested by the American Hospital Association, continue to be issued by HHS. Some regulations, including the highly unpopular Breach Notification Rule published August 24, 2009, have been withdrawn and reconsidered.

As recently as May 2011, a proposed rule was issued that would add two new rights for patients under the HIPAA Privacy Rule. The first permits patients to request and receive an accounting of disclosures that have been made of their PHI. The second would permit patients to access reports showing electronic access by both workforce members and persons operating outside the covered entity.

These most recent regulations will permit patients to have access to identifying information about the individuals who have accessed their PHI, and to detailed disclosures of how their PHI traveled from providers to individual staff employees and outside entities. This level of

transparency is required, according to HHS, in today's healthcare electronic records environment.

Healthcare providers opposing the new regulations contend that the benefits of transparency are far outweighed by the associated red tape and cost. The HHS counters that it must extend these privacy protection requirements to subcontractors in order to hold business associates fully accountable.

The HHS further asserts that without extending these protections to subcontractors, privacy protections for PHI can be avoided merely because a function is performed by an entity that is a subcontractor rather than a business associate having a direct relationship to the covered entity.

It is incumbent upon health law practitioners to protect your clients, whether covered entities, business associates or subcontractors, by ensuring that appropriate contractual obligations are in place.



Jeffrey A. Andrews is a shareholder and director with Vernon, Vernon, Wooten, Brown, Andrews & Garrett, PA, in Burlington, NC. He has more than 30 years experience in health law practice and issues representing hospitals, physicians, dentists and allied medical practices. In addition to health law and privacy issues, he works in such areas as commercial transactions, elder law, estate planning and asset protection, and intellectual property law. His JD is from the University of Virginia School of Law and he also has an undergraduate degree in Civil Engineering from the University of Virginia.

He has been a featured speaker at health law seminars statewide and frequently makes presentations on estate planning, health law, and business entity formation. He was recipient of the Citizen Lawyer award from the North Carolina Bar Association in 2007.

jandrews@vernonlaw.com