NELSON HARDIMAN
HEALTHCARE LAWYERS

Congratulations, you're a business associate?! The New Obligations and Newest Category of HIPAA Business Associates

I. BACKGROUND: AN OVERVIEW OF HIPAA

In 1996, Congress enacted HIPAA in order, among other purposes, to improve the efficiency and effectiveness of the health care system through the establishment of national and requirements for electronic health care transactions and to protect the privacy and security of individually identifiable health information. Collectively, these are known as HIPAA's Administrative Simplification provisions. The U.S. Department of Health and Human Services ("HHS") has issued a suite of rules, including a privacy rule and a security rule, to implement these provisions.

Under the HIPAA Administrative Simplification Rules (45 CFR 160, 162, and 164), subject entities – which are defined as "covered entities" – include health care providers who transmit health information in electronic form in connection with covered transactions. (45 CFR 160.103.) "Health care providers" include institutional providers of health or medical services, such as hospitals, and non-institutional providers, such as physicians and other practitioners, along with any person or organization that furnishes, bills, or is paid for health care in the normal course of business. "Covered transactions" are those for which HHS has adopted a standard, such as health care claims submitted to a health plan. (45 CFR 160.103 (definitions of "health care provider" and "transaction") and 45 CFR 162, Subparts K-R.)

II. WHO IS A BUSINESS ASSOCIATE?

The Privacy Rule, one of four HIPAA Administrative Simplification Rules, establishes requirements for covered entities with regard to non-employee "business associates." These are non-employees whose relationship with covered entities requires sharing of individuals' health records and other identifiable health information (collectively, "protected health information" or "PHI"). A "business associate" is defined as a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. (45 CFR 160.103.) The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. These include, among other things, arranging, performing, or assisting in such functions as data analysis, processing or administration, billing, and practice management (which necessarily involve PHI), or providing services to a covered entity through which individually identifiable health information is disclosed, such as legal, accounting, consulting, management, administration, accreditation, or financial services. The Privacy Rule permits a covered entity to disclose PHI to a business associate if satisfactory written assurance is obtained that the business associate will use the information only for the purposes for which it was engaged, will safeguard the information from misuse, and will help the covered entity comply with certain of its duties under the Privacy Rule. Prior to February 2010, the requirements were, in practical terms, limited. Business associates would sign business associate agreements ("BAA's") with covered entities agreeing to establish that they would safeguard the information. Covered entities had thereby satisfied their responsibility. That changed in February 2010, when the Health Information Technology for Economic and Clinical Health ("HITECH") Act (adopted in February 2009) took effect.

III. WHY IT MATTERS MORE TO BE A BUSINESS ASSOCIATE AFTER THE HITECH ACT

Before the HITECH Act, business associates were only indirectly subject to HIPAA. Effective February 18, 2010, business associates became directly responsible for HIPAA compliance and subject to civil and criminal penalties for noncompliance. (42 U.S.C. 1320d-5 and 1320d-6.) HITECH dramatically increases the obligations of business associates far beyond the days of entering into a BAA, and makes them directly accountable under the HIPAA Privacy Rules. Among other requirements, HITECH requires business associates to comply directly with another of the HIPAA Administrative Simplification Rules, the Security Rule, which requires implementation of administrative, physical and technical safeguards for electronic protected health information (“e- PHI”); and developing and enforcing related policies, procedures, and documentation standards, including designation of responsible personnel. (42 U.S.C. 17931(a); 45 C.F.R. 164.308-312 and 164.316.)

Some categories of businesses that work with health care providers will have to assess whether or not they are business associates. The decision as to whether a party is a business associate has significant implications. Acknowledgment of business associate status when it does not apply can result in unnecessary exposure to civil and criminal penalties (42 U.S.C. 1320d-5 and 1320d-6); on the other hand, failure to enter a business associate agreement when one is required violates HITECH. (42 U.S.C. 17932(b) and 17934(c).)

Some businesses have argued that the services that they provide to healthcare providers do not qualify for business associate status by virtue of their relationship to the information or the provider. In a guidance document issued in December 2002, the Office of Civil Rights clarified that HIPAA does not require a covered entity to enter into a business associate contract with a person or organization that acts merely as a conduit for protected health information (e.g., the US Postal Service, certain private couriers and their electronic equivalents). A conduit transports information but does not access it other than on a random or infrequent basis as may be necessary for the performance of the transportation service, or as required by law. Since no disclosure is intended by the covered entity and the probability of exposure of any particular protected health information to a conduit is very small, we do not consider a conduit to be a business associate of the covered entity.

65 Fed. Reg. 82462, 82476.

The Office of Civil Rights has explained that “since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.” (OCR HIPAA Privacy Guidance, “Business Associates,” Published December 3, 2002. Available at: http://www.umkc.edu/ors/hipaa/docs/OCR05_BusAssoc.pdf.) Some entities have focused on the definitional term that a business associate acts “on behalf of the covered entity to argue that they are not business associates. For example, Microsoft and Google, the purveyors of Internet-based personal health record (PHR) platforms populated with PHI, have argued that they are not business associates because their platforms provide services to consumers, not covered entities. (See Adam Green, Health IT Policy Committee’s Privacy and Security Tiger Team, transcript available at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_12083_913626_0_0_18/2010-07-09-tigertranscript.Pdf.)

Some business that perform business associate-type functions may also question whether the particular healthcare provider they work with falls under the definition of covered entity set forth in Title 45, CFR Section 160.103. For example, providers who do not bill for any of their services electronically may not be covered entities.

For attorneys, accountants, consultants and others who work with healthcare providers on a regular basis, these arguments are of no avail. Professional services rendered by for health provider clients are likely to fit squarely within the definition of the business associate under Title 45, CFR Section 160.10. In addition, it is a safe bet that, in 2010, most health care providers are covered entities by virtue of their billing practices. The last question is whether the information transmitted by these providers constitutes protected health information (“PHI”) subject to HIPAA requirements. PHI includes, among other things, any information that is “created or received by a health care provider” and “[r]elates to the past, present, or future physical or mental health or condition of an individual; [or] the provision of health care to an individual[.]” If these conditions are satisfied, it is time to comply with the obligations of the business associate.

IV. WHAT IT MEANS TO BE A BUSINESS ASSOCIATE AFTER THE HITECH ACT

Once you’ve concluded that you are a business associate under HIPAA, you are required to enter into the BAA — business associate agreement — to provide access to PHI for the subjects of that information, allow for amendment or correction, and assist in accounting for PHI disclosures. (45 CFR 164.504(e)(2)(i)-(iii).) The practical consequences of being a business associate outlined in a post-HITECH BAA include:

- Direct compliance with HIPAA's business associate safeguards (42 U.S.C. 17934(a)), including limiting use and disclosure of PHI as specified in the agreement or as required by law, facilitating access, amendment and accounting of disclosures ("breach notification"), opening books and records to HHS for compliance audits, and returning or destroying PHI, if feasible, upon contract termination (45 C.F.R. 164.504(e));
- Direct compliance with the HIPAA Security Rule provisions directing implementation of administrative, physical and technical safeguards for electronic protected health information ("e- PHI"), and development and enforcement of a compliance plan encompassing related policies, procedures, and documentation standards.
- Among other compliance plan requirements, business associates now need to:
  - designate a security official;
  - initiate workforce training programs;
  - implement breach notification detection systems; and
  - prepare disaster relief plans.

(42 U.S.C. 17931(a); 45 C.F.R. 164.308-312; and 164.316.)

The requirements are both procedural and technical. For example, in order to comply with the Security Rule's requirement of notification of any breach of unsecured electronic PHI, many entities are disallowing public Internet email transmissions of PHI-which are, by definition, insecure and create a risk of breach notification-and instead electing to store and transmit information in an encrypted form, so that no notification is required, even in the event of a breach.

In addition to the foregoing requirements, business associates are all subject to other requirements, including, among other things, prohibitions on sales of PHI (42 U.S.C. 17935), restrictions on marketing and fundraising restrictions (42 U.S.C. 17936), and enhanced civil and criminal penalties for noncompliance. (42 U.S.C. 17939(a); 17931(b); 17934(c).) Potential liability if the business associate learns of a "pattern of activity or practice" by a covered entity that breaches their business associate agreement and fails to cure the breach, terminate the agreement, or report the non-compliance to HHS. (42 U.S.C. 17934(b); 45 C.F.R. 164.504(e)(1)(ii).) HHS, in turn, is required to audit business associate compliance. (42 U.S.C. 17940)

V. COMING SOON: BUSINESS ASSOCIATES OF BUSINESS ASSOCIATES

Although most provisions of the HITECH Act became effective February 18, 2010, the final rule implementing the modifications to the HIPAA Rules has not yet taken effect. In that time period, the requirements imposed on business associates have continued to undergo expansion.

On July 14 2010, HHS published formal notice of the proposed rule, which will not take effect until 180 days after final regulations are published. When finalized, the rule will require action by covered entities, business associates, and their subcontractors. Among other things, the proposed rule clarifies the obligations of business associates. It will require business associates to enter into their own business associate agreements with subcontractors, who will be directly subject to HIPAA (45 CFR 164.532) and to comply with the "minimum necessary rule," which generally requires that any use or disclosure be limited to the minimum amount of PHI necessary to perform the task at hand.

This notion that business associates will now have their own business associates-who are, in turn, bound by the business associate obligations delineated above-is yet another broadening change. Currently, business associates are required to ensure that subcontractors receiving PHI agree "to the same restrictions and conditions that apply to the business associate with respect to the [PHI];" After the final rule takes effect, subcontractors of professionals who service healthcare providers, such as expert witnesses retained by attorneys, will be required not only to sign BAA's, but to implement their own compliance plans!

The expansion of who is a business associate is only one of many new aspects of HIPAA compliance under the proposed rule. Most of the new elements represent additional stringencies, including a clarification that the absence of a BAA does not relieve an entity who meets the definition of a business associate from compliance. At the same time, there are a few bright spots. For example, the proposed rule creates a transition period in which pre-HITECH BAA's do not need to be amended. (45 CFR 160.501, 45 CFR 164.504(e).) If a business associate has an existing BAA that complies with the prior provisions of the HIPAA (i.e. post-February 2010), and its contract with a covered entity is not renewed or modified prior to the compliance date of the final regulations, then the new regulation allows the business associate.

NELSON HARDIMAN
HEALTHCARE LAWYERS

VI. CONCLUSION

Take the time to assess whether you are a business associate of a covered entity (or a business associate of a business associate). If you're the former, it's time to start planning for compliance. I've included an outline of steps towards compliance. While the requirements may appear cumbersome, they are part of the new regulatory landscape. It pays to take them seriously, and to start thinking and acting like a HIPAA-compliant entity. For questions on what your compliance plan should look like, you can visit http://www.cms.gov/hipaageninfo/ or stay tuned for the forthcoming "Congratulations, you're our HIPAA Compliance Officer?!"