Inside Counsel
January 20, 2017

Managing Business Associates in the HIPAA World

The cost of compliance is a primary factor in motivating vendors to shun being a Business Associate ("BA").

By Joseph A. Dickinson

Joseph A. Dickinson is Counsel in the Privacy & Data Security group at Tucker Ellis LLP. He is a litigator and counselor with more than 25 years of business and legal experience representing and advising corporations and senior leadership nationally and internationally. Joe has broad experience in the areas of data privacy and security, data breach litigation, HIPAA compliance, intellectual property litigation, and technology licensing. He can be reached at joe.dickinson@tuckerellis.com.

Like any compliance program, a robust program for managing Business Associates ("BA") isn't something you should find and copy from the Internet or create through simply attending seminars and conferences – yet many programs today are developed by smart people who begin their indoctrination in just these ways.

Having spent a significant part of my 23-year legal career focusing on issues related to data privacy and security and the last six years focused almost exclusively on these issues in healthcare, I've learned that there is no substitute for "living it."

The best programs are not based on documentation created from standard lists and commonly used forms; they are developed based on an understanding of the legal requirements, coupled with accurately documenting the organization's unique circumstances and regularly reviewing and revising the program to reflect both.

I've seen those programs which incorporate policies and procedures that refer to departments and job titles that don't exist and describe audit schedules when no audits are conducted. These programs end up being their own worst enemy.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[1] sets forth the obligations for those entities subject to the HIPAA regulations to protect the privacy and security of protected health information ("PHI"). HIPAA applies to Covered Entities, which include healthcare providers, healthcare clearinghouses, and health plans, as well as BAs.

The definition of "Business Associate" (45 C.F.R. §160.103) – one of the longest definitions in the regulation was expanded by the HIPAA Omnibus Final Rule ("Omnibus")[2] to include health information organizations, E-prescribing gateways, and other persons that provide data transmission services where the provision of that service requires access to PHI on a routine basis. A key area of concern relates to what is meant by "access."

The Department of Health and Human Services Office for Civil Rights ("OCR") has provided guidance that reinforces the notion that it is a very broad term. It includes having access to data even when that data is encrypted and the entity does not have access to the decryption key.

Prior to HITECH and Omnibus, BAs became obligated to comply with the HIPAA regulations as a result of the Business Associate Agreement ("BAA") entered into between the BA and the Covered Entity. HIPAA has always required that Covered Entities enter into BAAs prior to disclosing PHI to vendors who meet the definition of BA.

Since HITECH and Omnibus, BAs are directly liable for compliance with the HIPAA Security Rule, Breach Notification Rule, and portions of the HIPAA Privacy Rule. Of concern has been the fact that many vendors have sought to avoid being considered a BA as a business strategy to avoid the significant costs associated with HIPAA compliance.

This reluctance has also created an environment where Covered Entities struggle to convince vendors that they are BAs and to enter into the appropriate BAA.

The cost of compliance is a primary factor in motivating vendors to shun being a BA. BAs are required, among other things, to perform risk assessments, have risk management programs in place, have policy and procedures that address the privacy and security of PHI, and enter into a BAA with all of their subcontractors and vendors who also have access to PHI.

Given this environment, what can covered entities and BAs (who engage subcontractors who also meet the definition of a BA) do to manage the relationship from the initial engagement through termination? What are the key considerations for on-boarding a BA, managing the relationship, auditing the BA's compliance with HIPAA, and the key risks and potential liabilities associated with not properly managing them?

For purposes of determining who really is a BA, caution is the better part of valor. With each new update to the HIPAA regulations, the definition of "Business Associate" expands. Consequently, anyone representing a Covered Entity or a BA should implement thorough assessment procedures for determining the

Continued on back

scope of the relationship.

Guidance is available and, in particular, OCR provides guidance and a tool to determine whether a vendor is a BA. The significant penalties associated with not complying with the HIPAA rules and regulations governing BA relationships create an environment that strongly supports erring on the side of inclusion.

When it comes to PHI, understanding and managing the data flow is critical. When considering a relationship with a vendor, an adequate assessment of the flow of PHI should be step one. The checklist approach is common, but that process is not without concerns.

Checklists do not always accurately reflect the specific circumstances of the organization involved. In particular, the HIPAA-required risk analysis should play a key part in the due diligence associated with any new or renewed relationship.

Whether one uses a checklist or other tool for conducting due diligence, certain key information must be obtained. Any reluctance on the part of the potential BA for sharing this information should be a red flag and source of potential concern that may mean finding a different vendor.

Historically, many vendors have sought to avoid being labeled as BAs because of the increased obligations to protect PHI. Since High Tech and Omnibus, it no longer matters whether the vendor agrees to enter into a BAA.

The determination rests entirely with the OCR and the regulations. If it is determined that the service the vendor provides creates a relationship where the vendor meets the definition of a BA, then that vendor is a BA regardless of the existence of an appropriate BAA. Moreover, not having a BAA in place creates additional risk, as it is required under HIPAA for all BAs.

BAs should be required to provide, among other things, a data map or other tool for documenting the uses and disclosures of PHI; a risk analysis of the BA's security that has been implemented to protect the confidentiality, availability, and integrity of electronically stored PHI; and documentation related to the assets of the BA – in particular, the assets that will be used to access, process, store or otherwise use or disclose PHI.

Alternatively, the covered entity can ask the BA to certify that it has conducted a thorough and accurate risk analysis and is otherwise in compliance with HIPAA; however, this approach may not be reasonable if the covered entity is aware of circumstances that bring this compliance into question.

In managing BAs, having a flexible, living, breathing program is critical. Managing BAs requires far more than well-drafted policies and procedures; it requires evidence of having an organizational culture that prioritizes the privacy and security of PHI.

Many organizations have historically not adequately addressed this responsibility. Managing BAs should include an appropriate BAA, adequate audit procedures, training, regular evaluations of the current status of relationships so as to enable termination of access to and the return of PHI when the business relationship ends, and a thorough inventory of the organization's BAs. The BAA should include terms that require the BA's proactive involvement in implementing these components.

Rather than simply demand compliance, Covered Entities should seek to partner with their BAs since many lack adequate HIPAA compliance programs for various reasons, including insufficient resources, being new to the health care environment, and not fully appreciating their obligations.

As the definition of the BA continues to expand, the importance of this partnering becomes imperative, especially with vendors such as cloud service provides and software application developers. Successfully managing BA relationships includes recognizing that many of an organization's BAs are new to the game and need help when it comes to identifying and managing the HIPAA-related risks.

Since Omnibus, it is clear that BA subcontractors that create, receive, maintain, or transmit PHI are likely also BAs. This creates multiple levels of risk. Considering the complexity of HIPAA compliance and the difficulty that large Covered Entities encounter in managing these obligations, the downstream risks created by BAs and BA subcontractors who are now themselves BAs continue to grow at alarming rates.

One cannot manage such risk without first appreciating its true breadth and depth. Far too often, resources are not available to adequately manage direct relationships, much less those for which the organization has no direct link. As a result, organizations must continually revisit the terms of their BAAs, audit processes, policies, and procedures and must strive to impress upon their business partners the importance of focused, documented efforts to identify and manage the risks.

Organizations must go beyond the contracting process and provide enhanced training and auditing to help create and support an organizational culture that prioritizes the privacy and security of PHI. And finally, organizations must undertake to adequately document this "culture" and the fact that their HIPAA compliance program includes prioritizing the engagement of business partners who also manifest such a culture.

The article originally appeared on InsideCounsel.com, at:
http://www.insidecounsel.com/2017/01/20/managing-business-associates-in-the-hipaa-world