On the HIPAA Hook

By Andrew Hicks, MBA, CISA, CCM, CRISC

Some healthcare business associates are still asking if HITECH-HIPAA impacts them. The answer is just as important to their affiliated healthcare providers.

Thousands of companies are now legally obligated to comply with the HITECH-HIPAA regulations because of their business associate status—thanks to changes enacted through last year's HITECH-HIPAA Omnibus Final Rule. The change has left many third-party vendors questioning whether or not they are a business associate and must comply.

The responsibility—and worry—isn't just on the vendors. Covered entities (CEs) like hospitals and doctor's offices are also "on the hook" for ensuring their business associates are compliant to avoid reputation and brand damage that could come with a privacy or security breach incident, as well as resultant penalties from the Office for Civil Rights (OCR)—the HIPAA enforcer. Healthcare organizations, whether they are CEs or large business associates that need to manage subcontractors, must be concerned about the vendors that make up their supply chain. Almost every company in today's world is part of a digitally connected ecosystem of organizations including upstream customers and downstream vendors. As a result, HIM professionals and the healthcare industry at large need to ask important questions when it comes to the new HITECH-HIPAA laws, such as: Who's looking at my data? What are they doing with it? Is it properly secured? What am I liable for?

Organization Reputations at Risk

While these are indeed issues that IT security professionals at CE organizations are concerned with at the moment—even if they may not be liable for a breach and hence required to pay associated fines and penalties—they are also concerned with the impact on their organization's brand. Consider the recent breach associated with Cottage Health System in California. One of Cottage Health's business associates removed security protections that resulted in 32,500 patient records being exposed on Google. While Cottage Health is presumably concerned about the privacy of its patients, since the incident was not a lapse in its internal security, it can be assumed that they were also very concerned about their reputation in the healthcare community due to this incident. While this particular example shines a light on the complexities of business associate liability under the HITECH-HIPAA Omnibus Rule, it is easy to understand why the concern is on reputation when the finger can justifiably be pointed in another direction. The reason for this phenomenon is simple.

A breach can destroy the trust that exists between IT security professionals and their own companies, between the company and their customers/patients, and between the company and business partners. This concept moves the business associate compliance topic up the agenda, fairly and squarely, and onto the plate of the compliance officer/risk officer and the chief financial officer at any healthcare organization, since a breach and resulting harm of trust could in turn impact stock price and revenue. These are the concerns that privacy and security consultants are beginning to see, moving a long way from just the issue of a security breach. Now the focus is on "What does this really mean for my business?"

Various Ways Exist to Determine Status

Again, some organizations may not know they are a business associate that is required to implement certain HIPAA privacy and security regulations by the already-passed deadline of September 23, 2013. Prior to the final HITECH-HIPAA Omnibus Rule, business associates were only "contractually" liable for complying with HIPAA. In other words, if their upstream covered entities were not forcing their signature on a business associate agreement, these organizations escaped the mandate to implement the required administrative, physical, and technical HIPAA controls. More importantly, these organizations fell outside the scope of OCR's random audits in 2012, as well as any threat of civil and criminal penalties. Suffice to say, unless someone told you that you were a business associate or you had internal awareness of your classification as such, you likely didn't know anything about HIPAA or how it applied to your organization.

Fast forward to 2013 and the enactment of the final HITECH-HIPAA Omnibus Rule by the Department of Health and Human Services (HHS). As Leon Rodriguez, director of OCR, stated in a HHS press release, the Omnibus Rule imposed "sweeping changes" by making business associates and their subcontractors fully liable for providing proof of non-negligence in the case of a breach to avoid fines and penalties upward of $1.5 million. This is because all business associates are now fully liable for complying with HIPAA. And to make it clearer with regards to what sort of company constitutes a business associate, the Omnibus Rule provided the following definition:

> A 'Business Associate' is generally a person or entity that creates, receives, maintains, or transmits protected health information (PHI) in fulfilling certain functions or activities for a CE. And health information that is created or received by a CE, identifies an individual, and relates to that individual's physical or mental health condition, treatment, or payment for healthcare is considered PHI when it is transmitted by or maintained in any form, including electronic media.

If an organization is still unsure about whether they are a business associate, the entity should consider the types of data that they create, receive, maintain, or transmit. PHI is the combination of individually identifiable information (i.e., name, address, Social Security Number) and any information that relates to the past, present, or future physical or mental health or condition of that same individual. Since business associates often manage data for a number of industries, they may not be sure if they harbor PHI. In these cases it may be best to perform a data flow and mapping exercise. This can more accurately determine if an entity is a business associate under the new HITECH-HIPAA definition with confirmation of administrative procedures that meet HIPAA standards by identifying and documenting the data flow of PHI.

The goal is to document the data flow of PHI and identify the methods in which data is created, received, maintained, or transmitted during the course of business. Vendors need a process for gathering PHI and its data flow across their organization. This can be done manually with a hard-copy questionnaire, or it can be scalable for larger organizations by creating an online questionnaire.

Some PHI 'Conduits' are not HIPAA-Covered

Potential business associates need to determine whether they may be a "conduit." Because OCR declined to qualify every type of business associate, this emphasizes the necessity of performing a factual analysis in uncertain situations, guided by issues designed to meet the goals of HITECH-HIPAA. The new business associate definition clarifies that there can be entities that maintain PHI for a CE, such as a data storage company, that now must be compliant with HIPAA. And to make things even more complex, the HITECH-HIPAA Omnibus Final Rule states that certain subcontractor organizations are also considered business associates.

After some debate by OCR and potential business associates, OCR acknowledged that mere conduits do exist and are considered business associates. But what is a conduit? There's actually a very narrow "conduit" HIPAA exception for entities that only have transient possession of PHI for transmission purposes. This is why it is important for covered entities to know if a subcontractor creates, receives, maintains, or transmits PHI on behalf of a business associate—because if so, they are indeed a business associate.

The narrow conduit exception is intended to exclude only those entities providing mere courier services, such as the US Postal Service or United Parcel Service and their electronic equivalents like Internet service providers (ISPs) providing data transmission services. However, it should be noted that the conduit exception is limited to transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission.

By contrast, an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the PHI.

Covered Entities on the Hook for Business Associates

Many CEs and large business associates feel that off-loading PHI to downstream vendors eliminates their compliance requirements and level of risk. However, this is truly not the case. In fact, for the reasons noted in the Cottage Health example, CEs and business associates must perform due diligence and risk modeling on all downstream vendors where PHI is

involved. Furthermore, CEs should consider expanding on existing boilerplate business associate agreements by requiring proof of controls such as intrusion detection and encryption.

Additionally, these agreements should include "right to audit" clauses, as well as the identification of downstream vendors where PHI may flow. Does this sound like too much of an effort? Probably not—if an organization, like Cottage Health, is the one dealing with a business associate breach involving its patients' protected health data.

While business associate agreements are a must, there are technology-enabled solutions available—some even free—to help streamline the process and minimize the time and effort needed to ensure continuous compliance of all downstream vendors.

Andrew Hicks (andrew.hicks@coalfire.com) is the healthcare practice director with IT governance, risk, and compliance vendor Coalfire.

Article citation:
Hicks, Andrew. "On the HIPAA Hook" *Journal of AHIMA* 85, no.4 (April 2014): 36-38.