Are You Subject to HIPAA?

By Jenny Holt Teeter*

Jenny Holt Teeter is a director and shareholder with Gill Ragon Owen, P.A. who regularly assists employers with general employment law compliance issues and healthcare providers and long term care facilities with regulatory registration and compliance.

I. Introduction

In 2016 alone, multiple health care providers, health insurance plans and others have paid millions of dollars in settlement money to the Office of Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") for violating the Health Insurance Portability and Accountability Act ("HIPAA").[1] More than three years after HHS issued final regulations that require additional compliance efforts of covered entities and their business associates, OCR has dramatically increased enforcement of what is collectively known as the "Omnibus Rule."[2]

The Omnibus Rule reaches beyond patients and their health plans, healthcare clearinghouses, and certain health care providers, which in HIPAA parlance are collectively known as "covered entities." The Omnibus Rule also creates more stringent requirements for the business associates of covered entities. The Omnibus Rule defines a business associate as an entity that, on behalf of a covered entity, performs functions, activities, or services involving the use or disclosure of protected health information ("PHI").[3] Significantly, the Omnibus Rule makes certain provisions of HIPAA's Security Rule and Privacy Rule directly applicable to business associates.[4] Thus, business associates must comply with substantially the same HIPAA requirements as covered entities or themselves face fines.

Many businesses and service providers do not realize that they are business associates or recognize obligations related to their status. Many lawyers and accountants serve hospitals, physicians, dentists, and other healthcare providers and occasionally see protected patient information. While the lawyers recognize the importance of keeping such information confidential, they may not realize that, as a business associate of their covered entity client, they also are required to implement office-wide policies and procedures to systematically protect the PHI received from their client. Other service providers may not realize that their assistance with an employer's self-funded insurance plans may also create a business associate relationship because of the occasional disclosure of employee PHI. The business associate relationship could also extend to IT companies or storage companies who store information for a healthcare provider or company with a self-funded insurance plan, even though those companies never "access" the information. These service providers are required to comply with HIPAA whether or not they recognize themselves as business associates and could incur significant penalties for failing to do so.

"Many lawyers and accountants serve hospitals, physicians, dentists, and other healthcare providers and occasionally see protected patient information. While the lawyers recognize the importance of keeping such information confidential, they may not realize that, as a business associate of their covered entity client, they also are required to implement office-wide policies and procedures to systematically protect the PHI received from their client."

A. The Security Rule: Knowing Your Risk 101

Generally, the Security Rule requires covered entities and business associates to (i) ensure confidentiality, integrity, and availability of all electronic PHI (ePHI) they handle; (ii) protect against reasonably anticipated threats to the security and integrity of ePHI; (iii) protect against any uses or disclosures prohibited by the Privacy Rule; and (iv) ensure their workforce members comply with the Security Rule.[5] The Security Rule acknowledges that covered entities and business associates range in profiles, and it allows those entities to adopt policies and procedures that most appropriately address their size, technical capabilities, and financial position, giving due consideration to the probability and severity of the risk they posit to ePHI in their control. Lawyers and law firms often function as business associates and must adhere to the same compliance requirements as their clients, whether that client is a business associate or a covered entity.

An essential compliance component of the Security Rule is the requirement that business associates conduct an accurate and detailed risk assessment that evaluates the entity when it comes to confidentiality, integrity, and availability of ePHI.[6] Also, the Security Rule requires, among other things, that both covered entities and business associates select a "security official."[7] This Security Rule "guard dog" of sorts should be responsible for a host of tasks, including: developing and implementing the policies and procedures required under the Security Rule; overseeing security training to the workforce; enforcing appropriate screening procedures for the personnel that has access to ePHI; identifying backup technology that will provide an extra layer of protection in the event of a data breach; and properly encrypting ePHI. It is vital for a business associate or covered entity to adopt security management policies and regularly conduct risk analyses to avoid paying hefty penalties to the OCR.

B. The Privacy Rule: Protecting the Patient

The Privacy Rule originally only applied to covered entities, but with the inception of the Omnibus Rule in 2013, the Privacy Rule also applies to business associates that come in contact with PHI.[8] While the Security Rule addresses the required policies and procedures to protect the confidentiality and integrity of ePHI, the Privacy Rule regulates which disclosures and uses of PHI are permissible or required. Covered entities and business associates may use or disclose PHI only where it is both required by law and required or permitted by its business associate agreement. Under the "permissibility" umbrella, generally, business associates and covered entities must "make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[9]

Because business associates are now directly liable under the Privacy Rule, they must ensure proper safeguards are in place that limit the access to PHI by staff and that those safeguards are defined in their respective business associate agreements. For instance, lawyers or law firms acting as business associates must be careful to formulate its requests to covered entities for client PHI so only the minimum necessary disclosure is produced.

II. Lawyers as Business Associates: Are You Prepared?

HIPAA business associates do not come in one shape or size—business associates can include accountants, IT firms, lawyers, and law firms. A lawyer or firm falls within the definition of a business associate if the lawyer "provides, other than in the capacity of a member of the workforce of such covered entity, legal . . . services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of PHI from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person."[10] Under the Omnibus Rule, a subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate also falls within the definition of a business associate. As explained in the discussion preceding the Omnibus Rule, "a person becomes a business associate or subcontractor by definition, not by the act of contracting with a covered entity or otherwise." In other words:

- If you or your firm provides professional legal services to a covered entity that involves the disclosure of PHI to you or your firm, then you might be a business associate.
- If you or your firm provides professional legal services to a business associate of a covered entity and you create, receive, maintain or transmit PHI on behalf of the business associate, then you might be a subcontractor of the business associate.[11]

Due to the expanded definition of a business associate and the direct liability the Omnibus Rule attaches to a business associate, it is crucial for you to ask yourself if you or your firm falls into one of these categories.

One important change is the addition of "subcontractor" to the definition of a business associate. Prior to the Omnibus Rule, a business associate's (or subcontractor's) obli-

gations were born of the contract terms of a business associate agreement entered into with a covered entity (or in the case of a subcontractor, the agreement entered into with a business associate) to not use or disclose PHI in an impermissible way. Now, business associates and subcontractors are not only subject to contractual liability but are also directly liable for noncompliance under HIPAA.[12] A business associate must abide by the Security Rule and the Privacy Rule and enter into a business associate agreement ("BAA") with the subcontractors it hires.[13]

Unfortunately, the farther removed you are from the covered entity, the less obvious it becomes as to whether or not you fall within the expanded definition of a business associate. Nonetheless, it is a business associate's obligation, *not* the covered entity's, to ensure a business associate and subcontractor enters into a proper business associate agreement. It is important to note two things. First, the lack of a contract between two parties does not prevent "subcontractor designation" by OCR, and, thus, does not prevent liability in the absence of a business associate agreement. Second, lawyers and law firms still must recognize third-party relationships that trigger the need for a business associate agreement no matter how far down the chain the PHI flows because all contractors and subcontractors are business associates if they create, maintain, or transmit PHI.[14]

III. Enforcement on the Rise—Business Associates Face Penalties

Notably, the enforcement provisions of the Omnibus Rule no longer reserve civil money penalties for non-compliant covered entities.[15] Under the HIPAA Enforcement Rule, business associates and their subcontractors are directly liable for particular HIPAA violations caused by their own noncompliance as well as violations caused by their respective *agents*.[16] Prior to the inception of the new regulations, covered entities could not be held liable for their business associates' HIPAA violations if a proper business associate agreement was in place and both did not know of the breach of the agreement or terminated the agreement or reported the breach to HHS if steps to cure the breach were unsuccessful. Covered entities and business associates can now be held liable for the acts or omissions of its business associates or subcontractors that are acting as "agents," as determined under the federal common law of agency. Importantly, as mentioned earlier, the mere existence of a business associate agreement will no long indemnify a covered entity or business associate for its respective business associate or subcontractor's acts or omissions in violation of HIPAA.

Penalties are capped at $1.5 million per year for each type of HIPAA violation (from an individual who did not know and by exercising reasonable diligence would not have known that he/she violated HIPAA to an individual who violated HIPAA due to willful neglect that was not promptly corrected), but this amount could substantially increase depending on the number of individuals affected and the number of violations.

Enforcement actions are on the rise and significant monetary penalties have already been imposed this year.

•North Memorial Care of Minnesota agreed to pay a $1,550,000 settlement for failing to enter into a business associate agreement with a major contractor and failing to conduct an adequate risk analysis to evaluate the potential vulnerabilities to its patients' information, which is required under the Security Rule. Before North Memorial settled, the Attorney General of Minnesota brought allegations against the business associate for its own HIPAA violations. The AG and the business associate eventually settled for over $2 million and the business associate was forced to shut down for two years.

•A North Carolina orthopedic clinic agreed to pay $750,000 to settle charges that it handed over PHI to a potential business partner without executing a business associate agreement. In response, Jocelyn Smith, Director of the HHS, said, "HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise."

•Feinstein Institute for Medical Research agreed to pay a whopping $3.9 million dollars, the second-largest HIPAA penalty to date, to settle charges that its security management process was limited in scope, incomplete, and insufficient to address potential risks to the confidentiality of ePHI. OCR's investigation began after the covered entity filed a breach notification when an employee's laptop was stolen from his car.

These cases are only the beginning as OCR has launched Phase Two of its HIPAA audits, which will be conducted randomly to assess a covered entity or business associate's compliance with the Privacy, Security, and Breach Notification Rules. Even if your organization is not selected for a Phase Two Audit, preparing for one can help improve HIPAA compliance. These audits will likely become a permanent feature of OCR's investigatory authority, so it is important to determine now if data safeguards and security policies are sufficient to respond to a data breach and if those policies and procedures are appropriately documented in necessary Business Associate Agreements.

IV. What should a business associate agreement include?

A HIPAA BAA is a contract that works to protect PHI in accordance with HIPAA guidelines. HIPAA has always required covered entities to enter into a BAA with their business associates. Now, under the Omnibus Rule, business associates are also required to enter into BAAs with their subcontractors, first degree subcontractors with their subcontractors, and so on down the line.[17]

Familiarity with HIPAA regulations will help you in executing a thorough and compliant BAA that is tailored to the particularities of the parties' needs. A general covenant that each party will comply with HIPAA regulations is insufficient to form a satisfactory and enforceable BAA. When it comes to what to include in an agreement, here are a few tips:[18]

•**Be thorough.** Prevent disclosure of PHI by defining in the contract how and for what purpose PHI will be used or disclosed.

•**Prepare for breaches, security incidents, and cyberattacks.** Indicate in the agreement the time frame that business associates are expected to report a security incident, breach, or cyberattack. The quicker the incident is reported, the faster harm can be mitigated.

•**Identify what an incident report should contain.** A business associate agreement should contain the type of information it should provide in a breach or security incident report. The report should include:

- Name of the business associate and its contact information.
- Description of the breach, including the date of the incident and the date

of discovery, if known.

- Description of the type of PHI that was involved in the incident.
- Explanation of how the business associate is investigating the incident and protecting against any further incidents.

•Include an indemnification provision. Because the Omnibus Rule enforces penalties for noncompliance for business associates based on the acts/omissions of their subcontractors, consideration should be given to including indemnification provisions.

•Conduct workforce training. Ensure the workforce is properly trained on all security policies and procedures, including incident reporting. Provide periodic awareness training in order to keep the workforce up-to-date. Elect an individual to serve as a "security officer" to head up security management policies and procedures and risk assessments.

• Require Cyberliability Insurance.

V. Other Considerations for Law Firms

It is important to ensure that your firm's BAA (for the firm and/or its clients) has been updated to reflect the new compliance requirements of the Omnibus Rule. In April of 2016, HHS addressed the most commonly investigated compliance issues: impermissible uses and disclosure of PHI; lack of safeguards of PHI; lack of patient access to their PHI; use or disclosure of more than the minimum necessary PHI; and lack of administrative safeguards of ePHI.[19] Covered entities and their business associates continue to suffer hefty consequences for their non-compliance more than three years after the final rule's inception.

It is also necessary to identify whether your firm is a business associate or subcontractor of a covered entity and identify any of the firm's potential business associates and subcontractors. If PHI has been obtained by your firm, in addition to having a BAA with the client who gave you the PHI, you might need to execute a BAA with the subcontractors that create, receive, maintain, or transmit PHI on your behalf. Take note that even third-party consultants who serve primarily a clerical purpose, such as record scanning, copying, storage, or destruction companies, could qualify as subcontractors. It is up to you, not the covered entity or business associate you represent or the subcontractor you hire, to orchestrate efforts to identify and record how information enters the firm in order to execute BAAs when necessary.

HIPAA can be a formidable regulatory gauntlet. The days of sluggish enforcement efforts of the OCR have come to an end. The likelihood that you or your client will face a HIPAA investigation or audit will continue to grow. Lawyers must maintain a good working knowledge of HIPAA compliance requirements to protect their clients and themselves.

Endnotes:

*The author would like to thank her law clerk Tess Stewart for assistance with the drafting of this article.

1. HIPAA was passed on August 21, 1996, with the goals of giving more Americans access to health insurance coverage and making the delivery of healthcare more efficient. In response to an evolving technological landscape, Congress mandated that HIPAA implement nationwide security and privacy measures to ensure the confidentiality of patient health information—referred to as the Security Rule and the Privacy Rule. HIPAA also established penalties for entities in violation of these rules—the Enforcement Rule.
2. In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the larger American Recovery and Investment Act. HITECH enforced fines and updated policy to encourage healthcare providers to use Electronic Health Records (EHR). Pursuant to HIPAA and HITECH, HHS issued final rules requiring additional compliance efforts of covered entities and business associates in 2013. Collectively, those final rules are known as the "Omnibus Rule" due to the large number of topics they cover.
3. *See* 45 C.F.R. § 160.103.
4. *See* 45 C.F.R. § 164.306 (stating the Security Rule is applicable to business associates); 45 C.F.R. § 164.502 (stating that the Privacy Rule is applicable to business associates).
5. *See* 45 C.F.R. § 164.306.
6. *See* Guidance on Risk Analysis, www.hhs.gov (explaining that conducting periodic risk assessments is the cornerstone of compliance with the Security Rule).
7. *See* 45 C.F.R. § 164.308(a)(2); *see also* 45 C.F.R. § 164.530(a)(2) (requiring covered entities and business associates to also designate a "privacy official" to ensure compliance with the Privacy Rule; the security official and the privacy official could be the same individual depending on the needs of the organization).
8. *See* 45 C.F.R. § 164.502.
9. There are some exceptions to the Minimum Necessary Standard that depend on who the disclosure is made to—the disclosure is made to the individual (the patient in most cases), to a health care provider for treatment, to the Secretary of HHS for investigative purposes, or when it is made according to an authorization. 45 C.F.R. § 164.502(b)(2).
10. *See* 45 C.F.R. § 160.103.
11. *See* 45 C.F.R. § 160.103(3)(iii) ("Business associate includes: (iii) a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.").
12. *Id.*; *see also* 78 Fed. Reg. 5591 (January 25, 2013).
13. Under the regulatory and statutory changes, a business associate is directly liable:

•for impermissible uses and disclosures of protected health information; *see* 45 C.F.R.

§ 164.502(a)(3).

•for a failure to provide breach notification to the covered entity when unsecured protected health information is lost or inappropriately accessed; *see* § 164.410.

•for a failure to provide access to a copy of electronic protected health information to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement); *see* § 164.502(a)(4)(ii).

•for a failure to disclose protected health information where required by the Secretary of the Centers for Medicare & Medicaid Services ("CMS") to investigate or determine the business associate's compliance with the HIPAA Rules; *see* § 164.502(a)(4)(i).

•for a failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; *see* § 164.502(b).

•for a failure to enter into business associat agreements with subcontractors that create or receive PHI on their behalf; *see* § 164.502(e)(1)(ii).

•for a failure to provide an accounting of disclosures of protected health information, and last, but far from least, for a failure to comply with the requirements of the Security Rule; *see* 76 Fed. Reg. 31426 (May 31, 2011).

•for a failure to comply with the requirements of the Security Rule; *see* Section 13401 of the HITECH Act (providing that the Security Rule's administrative, physical, and technical safeguards requirements in §§ 164.308, 164.310, and 164.312, as well as the Rule's policies and procedures and documentation requirements in § 164.316, apply to business associates).

14. Although the Final Rule recognizes the "conduit exception," HHS has made clear that the exception is narrow and only applies to those entities providing mere courier services. "[A] conduit transports [PHI] but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law." 78 Fed. Reg 5566.

15. The Omnibus Rule adds "business associate" to the following provisions of HIPAA's Enforcement Rule: 45 C.F.R. §§ 160.300; 160.304; 160.306(a) and (c); 160.308; 160.310; 160.312; 160.316; 160.401; 160.402; 160.404(b); 160.406; 160.408(c) and (d); and 160.410(a) and (c). This was done to implement those sections of the HITECH Act that impose civil monetary penalties on business associates for certain HIPAA violations.

16. *See* 45 C.F.R. § 160.402(c)(2) (reading, "A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.").

17. *See* 45 C.F.R. § 164.502(e)(1).

18. Also, sample provisions for a BAA have been published on the HHS website at, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

19. See http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html. ■