Who is a HIPAA business associate?

Rick L. Hindmand, Richard S. Cooper, James J. Giszczak, Dominic A. Paluzzi | Monday, January 9, 2017

A wide range of vendors and contractors that perform services or other functions for health care providers or health plans face substantial obligations and potential liabilities as business associates under the Privacy, Security and Breach Notification Rules (HIPAA Rules) issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Therefore, it is crucial for covered entities, as well as anyone performing services or functions involving protected health information (PHI) for covered entities or business associates, to identify all of their business associate relationships so they can take appropriate actions to comply with the HIPAA Rules. As we will discuss in this white paper, whether a service provider is a business associate under the HIPAA Rules will depend on the relationship of the parties, the nature of the services and whether the activities involve the use, disclosure, transmission, or maintenance of PHI.

Take action

All parties to any contract or other arrangement involving PHI in connection with the performance of services or functions by anyone (other than the covered entity's workforce) should review their arrangements to determine whether a business associate relationship has been or will be created, as well as whether a business associate agreement is in place and, if so, whether revisions are warranted. Business associates (as well as covered entities) need to take appropriate steps to comply with the HIPAA Rules.

Background

The HIPAA Rules allow covered entities to disclose PHI to business associates, and allow business

associates to create and receive PHI on behalf of the covered entity, subject to the terms of a business associate agreement between the parties. PHI is defined broadly to encompass individually identifiable health information relating to the health of an individual or to the provision of, or payment for, health care services. For purposes of the HIPAA Rules, a covered entity is a health care provider (such as a hospital, physician practice, laboratory or pharmacy) that transmits health information electronically in connection with billing or other transactions covered by the HIPAA administrative simplification rules, a health plan or a health care clearinghouse (such as certain medical billing companies that process and submit claims to health plans).

In general, an individual (other than a member of the covered entity's workforce) or organization that performs or furnishes any function, activity or service for or on behalf of a covered entity involving the use or disclosure of PHI is a business associate. The HIPAA Rules define a covered entity's workforce as employees, volunteers, trainees, and others acting under the covered entity's direct control, regardless of whether they are paid.

Historically, business associates were contractually required to maintain the privacy, and protect the security, of PHI as provided in their business associate agreements – that is, if they entered into a business associate agreement. But until recently, business associates were not subject to sanctions under the HIPAA Rules for noncompliance with their business associate agreements or HIPAA Rules.

The HITECH Act and Omnibus Rule

On Feb. 17, 2009, President Barack Obama signed into law the American Recovery and Reinvestment Act of 2009, which included the Health Information Technology for Economic and Clinical Health Act (HITECH). This expanded the HIPAA obligations and exposure of business associates by applying various HIPAA Rules directly to business associates, requiring business associates to comply with breach notification requirements and subjecting them to civil and criminal penalties for HIPAA violations. Nearly four years later, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) issued the Omnibus Rule, which amended the HIPAA Rules and took effect in 2013.

In addition to implementing various provisions of the HITECH Act by applying the HIPAA Rule obligations directly to business associates, the Omnibus Rule extended the business associate definition to new categories of business associates, including cloud vendors and other companies that store or transmit PHI, as well as subcontractors of business associates. The Omnibus Rule also required the amendment of business associate agreements to incorporate the new standards and expanded the potential liability of covered entities to include exposure for the acts and omissions of a business associate if the business associate is deemed to be an agent of the covered entity and the acts or omissions are within the scope of the agency.

Expanded business associate definition

The HIPAA Rules, as amended by the Omnibus Rule, define business associate as any individual (other than a member of the covered entity's workforce) or organization that either:

- Creates, receives, maintains, or transmits PHI on behalf of a covered entity or an organized health care arrangement for a function or activity regulated under the HIPAA administrative simplification rules, such as claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing.
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, if the service involves the disclosure of PHI.

Who is a HIPAA business associate?

The Omnibus Rule added the following new categories of business associates:

- Those who store or otherwise maintain PHI.
- Health Information Organizations (HIOs), e-prescribing gateways and others who provide data transmission services to a covered entity and require routine access to PHI.
- Anyone who offers a personal health record to individuals on behalf of a covered entity.
- Subcontractors of business associates, if (i) the business associate delegates to the subcontractor a function, activity or service that the business associate has agreed to perform for the covered entity, or for another business associate, and (ii) any of the delegated functions, activities or services involve the creation, receipt, maintenance, or transmission of PHI.

Though covered entities and business associates are required to enter into business associate agreements, anyone who performs services or functions that fit within the definition of business associate will be subject to the business associate obligations under the HIPAA Rules, even if no business associate agreement is signed. Therefore, business associates (as well as covered entities) have a proactive obligation to identify their business associate relationships and satisfy the HIPAA Rules in connection with those relationships.

Subcontractor business associates

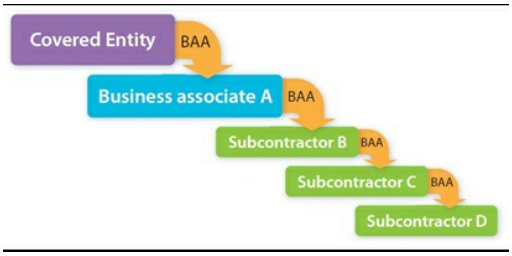
The expansion of business associate obligations to subcontractors was done to avoid a lapse of privacy and security protections when business associates share PHI with their subcontractors. Anyone, other than a member of a covered entity's or business associate's workforce, who assists a business associate in performing a function, activity or service involving PHI for a covered entity may potentially be subject to the HIPAA Rules as a subcontractor business associate.

A subcontractor may be deemed a business associate if at least part of a delegated task is within the business associate's responsibilities to the covered entity, although not all those who access PHI in providing services for a business associate will become business associates. For example, a business associate's disclosure of PHI for its (and not the covered entity's) management and administration would not create a subcontractor business associate relationship. However, the HIPAA Rules would still require reasonable assurances that the PHI will be held confidentially and will not be disclosed except as required by law or for the purposes of the disclosure, and agreement to notify the business associate if the recipient of the PHI becomes aware that confidentiality of the PHI has been breached. Moreover, a business associate will be allowed to use or disclose PHI for its management and administration only if the business associate agreement allows such use or disclosure.

HIPAA obligations and potential liability can extend to subcontractors who have no direct connection or relationship with any covered entity, no matter how far the PHI flows down the chain from business associate to subcontractors or how little the subcontractor knows about the relationship with the covered entity.

To understand how this works, consider the following scenario:

Business associate A engages subcontractor B to perform part of business associate A's responsibilities involving the covered entity's PHI. Subcontractor B in turn delegates some of its responsibilities involving the PHI to subcontractor C, and subcontractor C delegates part of its responsibilities to subcontractor D. In this case, subcontractors B, C and D (as well as business associate A) would all be considered business associates of the covered entity and the HIPAA business associate obligations would extend down the chain from business associate A to subcontractors B, C and D.



In these circumstances, business associate agreements would be required between:

1. The covered entity and business associate A
2. Business associate A and subcontractor B
3. Subcontractor B and subcontractor C
4. Subcontractor C and subcontractor D

The extension of business associate status to subcontractors can ensnare unsuspecting individuals and organizations because prior to the Omnibus Rule subcontractors were untouched by the HIPAA Rules.

Many could still be unaware that they are performing functions for covered entities or dealing with PHI.

Data transmission and storage

The Omnibus Rule added maintenance of PHI to the functions that trigger business associate status. For example, a data storage company that has access to PHI in either hard copy or digital form is a business associate even if the storage company never views the PHI or does so only on a random or infrequent basis. Before the Omnibus Rule, OCR had indicated that a document storage company would not be considered a business associate if the PHI was maintained in closed and sealed containers and the document storage company did not access the PHI (other than incidental access, such as when a box becomes damaged and needs to be repackaged). Now, a medical practice that stores old medical records in an off-site location needs a business associate agreement with the storage company.

With regard to data transmission services that trigger business associate status, the Omnibus Rule specifies two types of service providers: HIOs (i.e., organizations such as health information exchanges that oversee and govern the exchange of health-related information among organizations) and e-prescribing gateways. The definition also includes others who provide data transmission services to covered entities relating to PHI and require access to PHI on a routine basis.

OCR draws a distinction between data transmission services that require access to PHI on a routine basis and are therefore deemed to be business associates, and conduits, which are not business associates. This is a fact specific determination based on the nature of the services provided and the extent to which the service provider needs access to PHI to perform its data transmission services for the covered entity. OCR interprets the conduit exception narrowly and limits it to mere courier services, such as the U.S. Postal Service, UPS and their electronic equivalents, such as ISPs that provide mere data transmission services.

In light of the catch-all data transmission provision, the addition of maintenance of PHI as a business associate function, the Omnibus Rule preamble commentary and OCR's recent guidance on cloud computing (see below), the business associate definition now casts a wide net that can include service providers, such as cloud vendors, internet service providers (ISPs), application service providers (ASPs) and document storage companies that previously may not have been regarded as business associates.

Cloud service providers

In its October 2016 guidance on cloud computing, OCR confirmed that a cloud services provider that creates, receives, maintains or transmits electronic PHI (ePHI) on behalf of a covered entity is a HIPAA business associate even if all ePHI is encrypted and the cloud service provider does not have the encryption key. A cloud service provider that subcontracts to perform similar functions on behalf of the business associate involving ePHI is also a business associate.

OCR has specifically reminded covered entities and business associates that using a cloud service provider to maintain ePHI without entering into a business associate agreement violates the HIPAA Rules. In addition, risk analysis and risk management need to account for ePHI stored in the cloud, whether on servers within the U.S. or overseas.

OCR recognizes that in some cases a cloud service provider may not know that a covered entity or

upstream business associate is using the cloud service in connection with ePHI, and therefore may not be in a position to satisfy its business associate obligations under the HIPAA rules. The guidance clarifies that upon becoming aware that it is maintaining ePHI, a cloud service provider must comply with the HIPAA Rules or securely return the ePHI to the customer (or destroy it, if agreed). OCR notes that the 30 day period to correct noncompliance (in order to qualify for an affirmative defense under the HIPAA Rules) begins when the cloud service provider knows or should have known that a covered entity or business associate is maintaining ePHI in its cloud. OCR recommends that cloud service providers document their compliance, or their return or destruction of ePHI.

Business associates in the crosshairs

OCR's $650,000 settlement in June 2016 with a business associate, Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), demonstrated that it is serious about taking strong enforcement action and imposing severe penalties against business associates for failure to implement safeguards as required under the HIPAA Rules.

The CHCS settlement continued OCR's expansion of its enforcement focus on business associates, following a string of OCR settlements that held covered entities responsible for failing to enter into business associate agreements with their business associates or for failing to update a pre-Omnibus Rule business associate agreement.

It is also important to keep in mind that business associates are potentially subject to OCR's HIPAA audits. Moreover, state attorneys general and the Federal Trade Commission have also taken enforcement action against business associates.

Conclusion

A threshold issue in HIPAA compliance for any organization is identifying all of its business associate relationships, whether as a covered entity, upstream business associate or downstream business associate. In some cases this relationship may be apparent, and in other instances it may require some analysis. With expanded business associate obligations, scrutiny and related exposure, it is more important than ever to recognize all business associate relationships and ensure that appropriate safeguards are implemented.

Rick L. Hindmand

Richard S. Cooper

James J. Giszczak

Who is a HIPAA business associate?

Dominic A. Paluzzi