

## Business Associate Agreements Matter: Demystifying the Perceived Simplicity of HIPAA Agreements

August 21, 2024

*Holland & Knight Alert*

[Shalyn Watkins](#)

### Highlights

- Signing a Business Associate Agreement (BAA) is standard practice for most healthcare providers and businesses, but these parties sometimes do not read the agreement or even execute it as stated.
- BAAs are critically important, and how they are treated by affected entities can mean success or failure for a compliance program – especially in light of the Health Insurance Portability and Accountability Act (HIPAA).
- This Holland & Knight alert details several reasons why parties should always read, review and negotiate terms of a BAA prior to its execution.

---

For most healthcare providers and businesses, signing a Business Associate Agreement (BAA) is a standard practice. When contracting to provide services with an entity governed by the Health Insurance Portability and Accountability Act (HIPAA), it is a requirement that the entity enter into a business associate contract, also known as a BAA. This includes HIPAA covered entities, their business associates and downstream business associate subcontractors. However, parties often treat the agreements as boilerplate and either fail to read and negotiate their terms or, worse, forego executing the agreement altogether. Contrary to popular belief, though, BAAs are critically important and can make or break a compliance program if not taken seriously. Though it may seem easiest to simply sign a BAA as a standard attachment to a service agreement, this Holland & Knight alert will highlight five of the many reasons why parties should always read, review and negotiate the terms prior to execution.

### What Must a BAA Say?

HIPAA clearly outlines the required elements of a BAA, and the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) provides [sample agreements](#) on its website. Though this guidance is helpful, it is important to understand that the sample agreements represent the minimum requirements for BAAs. Pursuant to 45 CFR 164.504(e), a BAA between a covered entity and a business associate must:

- establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate
- provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or law
- require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI
- require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI
- require the business associate to disclose PHI as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and

# Holland & Knight

incorporate any amendments, if required) and accountings

- to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation
- require the business associate to make available to HHS its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule
- at termination of the contract, if feasible, require the business associate to return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity
- require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the business associate with respect to such information
- authorize termination of the contract by the covered entity if the business associate violates a material term of the contract; contracts between business associates and business associates that are subcontractors are subject to these same requirements

These elements must be included in all business associate agreements in order for the agreement to be considered valid.

## What Should Parties Consider When Negotiating BAAs?

BAAs should not be viewed as standard boilerplate. They require careful review and consideration by both parties.

1. **Noncompliant and Nonexistent Agreements.** Despite 45 CFR 164.314(a) and 164.502(e) clearly laying out the requirements for BAAs, many parties fail to comply to the basic formalities required under the regulations. Parties without experience working with covered entities often assume that standard confidentiality agreements or nondisclosure agreements will suffice. However, the failure to execute a BAA can result in severe monetary fines arising from multiple HIPAA violations. Disclosure of PHI in the absence of an executed BAA is an impermissible disclosure and potentially a breach requiring notice, as well as a violation of the regulation requiring a BAA.
2. **Old Form Agreements.** Some parties forget to update their BAAs as changes to HIPAA occur. For example, a form agreement that was originally drafted before 2013 would not address the HITECH Act omnibus rule, including the amended definition of a breach, and probably does not address the particular risks related to current operations of the contracting parties. Furthermore, as the OCR continues to promulgate new laws and regulations today, BAAs and HIPAA Policies and Procedures require updating. Holland & Knight has discussed many of these changes in its ongoing "OCR in Overdrive" alert series – view parts [1](#), [2](#), [3](#) and [4](#).
3. **Restrictive Agreements.** Since BAAs can include provisions beyond those required under the regulations, it is prudent that business associates read the additional provisions carefully to ensure they are not overly restrictive. The permitted conduct section of the BAA limits the business associate's ability to use or disclose PHI for only the purposes allowed in the agreement. But if that section is missing certain conduct, the business associate may be too restricted and incapable of providing services to the covered entity without violating HIPAA. For example, if a BAA does not include the use and disclosures of PHI for the business associate's own proper management and administration and to fulfill its legal responsibilities in the listing of permitted conduct, it will be difficult, if not impossible, for the business associate to comply with the terms of the agreement. BAAs are not "one-size fits all," and terms should be drafted carefully to ensure sufficient permissions for a business associate to perform its services.
4. **Unclear Reporting Obligations.** Some BAAs attempt to pass the covered entity's obligation to report breaches to

# Holland & Knight

the business associate. However, sometimes the business associate is not in the ideal position to effectuate such notices. It is important that business associates accepting this responsibility confirm their reporting obligations and ensure they have the infrastructure to report breaches to individuals, the Secretary of HHS and the media as required by law. Though a covered entity may delegate reporting obligations to a business associate, the OCR has been clear that the covered entity is ultimately responsible for ensuring that notice is provided in compliance with the breach notification regulations in HIPAA.

**5. Unrealistic Reporting Times.** When security incidents occur, business associates may not immediately be aware. Particularly in situations where the business associate works with independent contractors and parties outside its organization, the business associate is less likely to have immediate knowledge of security incidents and breaches. But if their BAAs require notification within days of the incident's occurrence, the business associate may be in breach of the BAA if it fails to timely report the incident to the covered entity. This creates an impossible situation for business associates, which could be avoided by reading and negotiating the reporting time obligations within the BAA. Though reporting must occur relatively quickly for the covered entity to assess whether a breach has occurred and if notification is required, business associates can request reasonable timing for reporting incidents at the outset.

Though this list is not exhaustive, it represents five of the biggest considerations for parties when entering into BAAs. HIPAA permits the addition of other terms that are not inconsistent with HIPAA. Provisions addressing indemnification, injunctive relief, relationship to state privacy laws and other federal laws – such as Part 2 Privacy and Cures Act information blocking, along with other terms – may be considered. The terms of these agreements can make or break a party's privacy compliance program and should be treated as important topics of negotiation instead of boilerplate.

For additional information, please contact the authors or another member of Holland & Knight's [HIPAA and Healthcare Privacy Team](#).

---

Information contained in this alert is for the general education and knowledge of our readers. It is not designed to be, and should not be used as, the sole source of information when analyzing and resolving a legal problem, and it should not be substituted for legal advice, which relies on a specific factual analysis. Moreover, the laws of each jurisdiction are different and are constantly changing. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. If you have specific questions regarding a particular fact situation, we urge you to consult the authors of this publication, your Holland & Knight representative or other competent legal counsel.

---



**Shalyn S. Watkins** is a healthcare attorney in Holland & Knight's Los Angeles office. Ms. Watkins represents various healthcare providers and companies, including, but not limited to, individual providers and provider practices, digital health platforms, emerging companies, laboratories, technology companies and behavioral health companies. She also assists clients with developing and managing compliant healthcare programs.

+1.213.896.2559 | [Shalyn.Watkins@hklaw.com](mailto:Shalyn.Watkins@hklaw.com)

## Data Centers and HIPAA Requirements

May 27, 2025

*Holland & Knight Cybersecurity and Privacy Blog*

[Shannon Britton Hartsfield](#)

Data centers may provide space, cooling, power, physical wiring and connectivity to customers that store hardware in the centers. If this hardware is used to store protected health information (PHI) subject to federal Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules, data center operators may have HIPAA responsibilities.

### HIPAA History Regarding Data Storage

HIPAA applies to "covered entities," "business associates" and "subcontractors." Covered entities include health plans, healthcare clearinghouses and most healthcare providers. Business associates include a number of different types of businesses that serve covered entities, as well as subcontractors that provide PHI-related services to business associates. Business associates conduct functions on behalf of a covered entity requiring the creation, receipt, maintenance or transmission of PHI. Entities that provide data transmission services involving PHI and that require access on a routine basis to such PHI are also business associates, raising a question as to whether HIPAA applies to data center operators.

Even though a data center may provide the same types of services to all of its customers, regardless of whether the customers are in the healthcare industry, HIPAA potentially applies to data centers serving customers that use the services for PHI-related purposes. The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) enforces HIPAA privacy and security regulations. Over time, OCR's position on the applicability of HIPAA to PHI storage has changed.

In 2003, OCR provided a letter to Tindall Record Storage, a Texas company, stating "that a business associate agreement is not required between a covered entity and a document storage company performing functions on behalf of the covered entity, where any protected health information released to the storage company is transferred and maintained in closed and sealed containers, and the document storage company does not otherwise access protected health information."

Applying that reasoning to a data center operator providing co-location or other services where no access to PHI is needed, it would seem that those services would not create a business associate relationship. However, subsequent changes to HIPAA and other informal guidance likely change that analysis.

### HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 expanded the application of certain HIPAA requirements to business associates. For example, the HIPAA security rule provisions now apply to business associates in the same way that they apply to covered entities. Additionally, business associates are required by law to comply with applicable privacy provisions of their business associate agreements with covered entities.

OCR finalized regulations in 2013 implementing certain HITECH Act requirements. In its preamble to those regulations, OCR changed its position from the guidance it provided in 2003 by referring to a record storage company that holds boxes of paper records on behalf of a covered entity but does not know the names of individuals whose information is stored in those boxes as a "business associate."

In 2016, OCR issued informal guidance on its website indicating that cloud service providers (CSPs) are business

# Holland & Knight

associates. OCR noted that cloud computing can take different forms and may involve access to networks, servers and storage.

In a frequently asked question regarding CSPs, OCR indicated that a CSP is a business associate if it processes or stores electronic PHI (ePHI). This is the case even if the ePHI is encrypted and the CSP has no decryption key. OCR indicated that encryption, by itself, would not eliminate the need for the CSP or the covered entity to address other safeguards such as disaster planning and physical safeguards for the systems and servers.

The covered entity, rather than the CSP, could be responsible for certain compliance obligations such as adhering to HIPAA's authentication requirements if the CSP has no access to the content of the PHI. If the CSP has no way to address a required HIPAA compliance obligation, this should be addressed in the HIPAA business associate agreement between the parties.

## HIPAA Obligations If a Data Center Is a Business Associate

If a data center meets HIPAA's definition of a business associate, it must implement an effective HIPAA compliance program. A business associate's HIPAA obligations include:

- assessing how PHI is stored and where it is maintained
- conducting and documenting an accurate and thorough risk analysis of the potential threats and vulnerabilities to electronic PHI and how those risks will be mitigated
- appointing or hiring a security official who is responsible for developing and implementing policies and procedures to enable the data center operator to comply with relevant HIPAA requirements
- training its workforce on the HIPAA policies and procedures relevant to their functions
- flowing down HIPAA business associate agreement requirements to subcontractors that have involvement with the maintenance of the PHI

Although data centers may have many physical and technical security measures in place, if those data centers will be serving HIPAA-covered entities or business associates, HIPAA will require the data center operator to comply with numerous requirements specific to these federal regulatory provisions.

For more information or questions, please contact the author or any member of Holland & Knight's [Data Center Team](#) or the [Data Strategy, Security & Privacy Practice Team](#).



**Shannon B. Hartsfield** is a health lawyer and the executive partner of Holland & Knight's Tallahassee office. Ms. Hartsfield's practice focuses on the intersection of healthcare delivery and regulation, with a particular emphasis on compliance, technology, digital health and privacy. She is Board Certified in Health Law by The Florida Bar Board of Legal Specialization and Education. She is a co-author of [HIPAA: A Practical Guide to the Privacy and Security of Health Data](#), Second Edition, in association with the American Bar Association (ABA).

+1.850.425.5642 | [shannon.hartsfield@hklaw.com](mailto:shannon.hartsfield@hklaw.com)