Reinhart

# HIPAA Tips for Start-Ups: Negotiating Business Associate Agreements

The first time you walk into a doctor's office you have to sign an acknowledgement that you received a copy of the practice's HIPAA Notice of Privacy Practices. But, does anyone ever read it (besides health care lawyers)? While HIPAA is definitely not a new acronym in your vocabulary, you may not have considered whether and how it impacts your start-up.

**POSTED:**

Jun 8, 2016

**RELATED PRACTICES:**

Health Care

https://www.reinhartlaw.com/practices/health-care

## What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It is a federal law that protects the privacy and security of individually identifiable health information—called "protected health information" ("PHI"). One of the most widely publicized purposes of HIPAA is to make health insurance more portable when employees change jobs. HIPAA, however, has much more far-reaching implications for the health information world. Its implementation caused the development of national standards for electronic health care transactions and code sets, unique health identifiers and security, and thereby served as a catalyst for today's proliferation of electronic medical records.

## Who Needs to Comply with HIPAA?

HIPAA covers two categories of individuals/entities: covered entities and business associates. Covered entities include health care providers, health plans and health care clearinghouses. These are the individuals/entities we generally think of when we think of HIPAA.

Business associates consist of individuals or entities that perform a service *on behalf of* a covered entity that involves creating, receiving, maintaining or transmitting PHI. Business associates include, for example:

- companies providing data analysis, practice management services or software to a covered entity;
- software companies exposed to PHI;
- cloud providers;
- e-prescribing providers;
- electronic health record vendors; and


All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.

- consultants, lawyers and accountants.

A business associate's subcontractor (*e.g.*, a software vendor's law firm) may also be a business associate. For example, a company that contracts with a business associate to perform a service that involves creating, receiving, maintaining or transmitting PHI on behalf of a covered entity is considered a business associate for purposes of HIPAA.

## You Are a Business Associate. Now What?

As a business associate, startups are required to comply with most of HIPAA's security provisions, as well as some of the requirements of HIPAA's privacy rule and breach notification rule. Note: Compliance is no walk in the park. Among other requirements, business associates are required to implement certain administrative, physical and technical safeguards to protect PHI (which include, for example, adoption of policies and procedures, and training of workforce members), to conduct an annual security risk assessment and to notify individuals of any breach of their PHI. A non HIPAA compliant business associate could face serious financial penalties. Equally daunting, a non HIPAA compliant business associate may lose customers and business partners as most covered entities are unwilling and unable to contract with business associates that fail to comply with HIPAA.

Business associates must also enter into a special type of contract—a business associate agreement—with each covered entity for which the business associate performs a service.

## What Are Business Associate Agreements?

A business associate agreement is generally a stand-alone agreement, distinct from (or an exhibit to) the main services or license agreements that the parties sign. That being said, business associate agreements are very important as they lay out each party's rights and responsibilities with respect to PHI. If not correctly negotiated, business associate agreements can be a source of great liability.

## What Is Required in a Business Associate Agreement?

HIPAA requires certain terms be included in a business associate agreement, and


All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.

sets the minimum threshold for those terms. For example, HIPAA requires that each business associate agreement provide that the business associate will:

- use appropriate safeguards and comply with applicable provisions of the Security Rule;
- report to the covered entity any unauthorized use or disclosure of PHI of which it becomes aware, including breaches of unsecured PHI and security incidents;
- ensure that any subcontractors that create, receive, maintain or transmit PHI on the business associate's behalf agree to the same restrictions and conditions that apply to the business associate with respect to such information;
- make available PHI to provide individuals with certain rights (*e.*, access, amendment, accounting)
- make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received on behalf of, the covered entity available to the secretary of the Department of Health and Human Services ("HHS") for purposes of determining the covered entity's HIPAA compliance; and
- upon termination of the business associate agreement, return or destroy all PHI unless doing so is infeasible, in which case the business associate must extend the protections of the business associate agreement and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

## Why Negotiate Business Associate Agreements?

While HIPAA determines the minimum threshold for the terms described above, there is room for negotiation. For example, the timeframes for reporting breaches or security incidents is often an area of negotiation. The same is true of timeframes regarding individual rights (access, amendment and accounting). HIPAA generally provides the maximum timeframes that must be included; however, covered entities often provide much shorter timeframes in their standard business associate agreements. As a business associate, startups should be careful not to overcommit (*i.e.*, you may not be able to provide breach notification to a covered entity within 24 hours if you use subcontractors as you will need to leave enough time for the subcontractor to notify you if the breach happens in the subcontractor's control). Further, some of the requirements related to individual rights may not be applicable if the startup is not maintaining a designated record set (*e.g.*, medical records or payor records) on behalf of the covered entity.


*All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.*

Other areas to consider include:

- **Audit Rights.** Just because the Secretary of HHS requires access to your books and records does not mean that a covered entity also needs access. Consider revising any such provision accordingly.
- **Indemnity.** If there is an indemnity provision, consider striking it completely or including a limitation of liability. This may depend on the leverage you have.
- **Reimbursement for Breach-Related Costs.** In addition to indemnity, many covered entities add a provision regarding reimbursement for breach-related costs. Again, you may consider striking this provision altogether or tailoring it so that it is more reasonable (*g.*, only includes actual costs of mailing notices).

## What about Subcontractors?

As described above, under HIPAA, each business associate must ensure that any subcontractors that create, receive, maintain or transmit PHI on the business associate's behalf agree in writing to the same restrictions and conditions that apply to the business associate with respect to such information. That being said, it may not be sufficient to simply repurpose the business associate agreement the business associate signed with the covered entity. Instead, careful consideration should be given to provisions containing timeframes to ensure that all parties are able to meet their obligations. For example, if a business associate is required to notify a covered entity of a breach within four days, the business associate may be unable to meet that requirement if the business associate also requires its subcontractors to notify the business associate within four days. Further, regardless of whether it is included in the original business associate agreement, you may want to consider including indemnification and reimbursement for breach-related costs.

Reinhart's Health Care team is available to assist you in reviewing your business associate agreements and addressing other HIPAA related issues. Please feel free to contact Nicole Dermer or any member of Reinhart's Health Care team, or your Reinhart attorney, to discuss your HIPAA related questions or concerns.

*These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.*


*All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.*