

PARSONAGE VANDENACK WILLIAMS LLC

"Focused Experience in Action"

5332 South 138th Street, Suite 100
Omaha, NE 68137
402-504-1300
www.pvwlaw.com

WHAT TO DO WHEN YOU ARE ASKED TO SIGN A HIPAA BUSINESS ASSOCIATE AGREEMENT

If your business is going to handle or have access to individual medical or health information in any form (i.e. paper, oral or electronic), for another entity such as an insurance company, hospital or medical practice, then that entity or its attorneys will probably ask you to sign a contract entitled "Business Associate Agreement" or "HIPAA Business Associate Agreement".

What is this contract? Why are you being asked to sign it? What are you being asked to agree to? This article addresses these common questions.

I. The Basics of HIPAA

The following are the basic terms and concepts that are critical to understanding the purpose of a Business Associate Agreement:

- "HIPAA" is the federal Health Insurance Portability and Accountability Act, which among other things protects the privacy of individual medical and health information.
- "HITECH" or the "HITECH Act" is the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009. HITECH was enacted to promote the adoption and meaningful use of health information technology. Subtitle D of HITECH addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
- A "Covered Entity" under HIPAA is either a "health plan," "health care clearinghouse" or a "health care provider," each of which has its own detailed definition under HIPAA.
- Your business will be a "Business Associate" of a Covered Entity under HIPAA if it performs certain functions or activities that involve the use or disclosure of "Protected Health Information" on behalf of, or provides services to, a Covered Entity. These functions and activities include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefits management, practice management, and repricing. Business associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial services.
- "Protected Health Information," or "PHI," is individually identifiable health information you receive from or create or receive on behalf of a Covered Entity.

II. What Is this Contract and Why Am I Being Asked to Sign It?

HIPAA requires that a Covered Entity have a written agreement with its Business Associate. This requirement is the legal driver behind what your counterparty is asking. The Covered Entity must, through such a written agreement, obtain “satisfactory assurance” from the Business Associate that the Business Associate will “appropriately safeguard” PHI the Covered Entity discloses to the Business Associate.

These agreements are customarily referred to as “Business Associate Agreements.” The remainder of this article assumes that your counterparty is in fact a Covered Entity and that PHI will in fact be disclosed to you. If your counterparty is not a Covered Entity and you will not have access to PHI, then your counterparty is not legally required by HIPAA to enter a Business Associate Agreement with you.

It is important to note that before the HITECH Act, the HIPAA privacy and security requirements applied only *indirectly* to Business Associates. Any privacy or security requirements were made applicable to Business Associates only through the use of a Business Associate Agreement. Under HITECH, many of the HIPAA standards apply directly to Business Associates, and Business Associates are now subject to the same civil and criminal penalties as Covered Entities.

III. What Am I Being Asked to Agree To?

HIPAA requires that the Covered entity impose certain specific obligations on you via the Business Associate Agreement. Under HITECH, these requirements are not only imposed via contract. Rather, HIPAA security standards that apply to health plans and health care providers also apply *directly* to Business Associates. There are important HITECH breach notification requirements that both Covered Entities and Business Associates must comply with. Covered Entities and Business Associates can delineate by contract how the notification requirements will be implemented in their Business Associate Agreements.

The following points summarize the minimum required obligations in a “standard” Business Associate Agreement. It should be noted that these points are only intended to give an overview of the requirements, not the full details, which are found in the federal regulations. Some of the required obligations are relatively straightforward. Some are more broadly worded and open-ended.

- You must report any unauthorized use or disclosure of the PHI to the Covered Entity.
- You must report any security incident to the Covered Entity.
- You must not use or further disclose the PHI other than as permitted or required by the agreement or as required by law.
- You must obligate your agents and subcontractors to agree to the same restrictions and conditions that apply to you, and they must agree to implement reasonable and appropriate safeguards for the protection of electronic PHI.

- You must make the PHI available in connection with individuals' rights under federal law to access their PHI. If you maintain an electronic health record, you must agree to provide such information in electronic format.
- You must make the PHI available for amendment and incorporate any amendments in connection with individuals' rights under federal law to seek amendment of their PHI.
- You must make available the information required to provide an accounting of disclosures of PHI to individuals in accordance with their rights under federal law to obtain such an accounting.
- You must make your internal practices, books, and records relating to the use and disclosure of the PHI available to the federal government for purposes of determining the Covered Entity's compliance with HIPAA.
- You must return or destroy all PHI, if feasible, at the termination of the agreement, or, if return or destruction is not feasible, you must continue to protect the PHI even after termination.
- You must agree to comply with the policies and procedures and documentation requirements of the HIPAA Security Rule.
- You must agree to report any access, use or disclosure of PHI not permitted by the Agreement, and any breach of PHI of which you become aware without unreasonable delay and in no case later than 60 calendar days after discovery.
- You must use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the agreement.
- You must implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI.

Typically, addressing the "open-ended" requirements involves such matters as password protecting computers, workstation security, data backup/disaster recovery plans, locked storage for paper PHI, sanctions for violating employees, etc. A more detailed analysis of what is adequate depends on a variety of factors such as the form of the PHI and the nature of the services you will be providing.

One other important requirement of a Business Associate Agreement is that it provide for termination by either party in the event of the other party's breach. A cure period is permitted, but the Covered Entity cannot legally waive breach indefinitely. The mandatory termination of the Business Associate Agreement can jeopardize your underlying contract and business relationship, because a Covered Entity cannot keep disclosing PHI to you without the required contractual assurances for its protection.

IV. Complying with Your Business Associate Agreement Obligations

Once you have entered a Business Associate Agreement, you should make sure your employees understand the importance of complying with it and exactly how it is you will comply. If you handle electronic PHI or handle PHI on any sizeable scale, you should have a simple,

straightforward HIPAA Business Associate Policy to use and facilitate compliance with your obligations. If a Covered Entity requests that you sign a Business Associate Agreement, you should review the agreement carefully to make sure that you fully understand your obligations under the agreement and are able and willing to comply with its terms.

