Why am I being asked to sign a HIPAA Business Associate Agreement?

Does your business handle or have access to individual medical or health information, in any form, for another entity - like Medicaid? You may be asked to sign a contract called a "Business Associate Agreement." This is a federal requirement of the Office for Civil Rights.

Here are some basic terms you need to know.

> **HIPAA** is the Health Insurance Portability and Accountability Act of 1996. HIPAA regulations protect the privacy of individually identifiable health information.
>
> A "**covered entity**" defined by HIPAA is either a health plan (like Medicaid), a health care provider (medical providers defined by the Social Security Act), or a health care clearinghouse, which assists providers in processing electronic transactions.
>
> Your business is a "**business associate**" of a covered entity if you create, receive, maintain, or transmit protected health information on behalf of, or provide services to a covered entity.
>
> "**Protected Health Information**" or PHI is individually identifiable health information which relates to the past, present, or future provision of care. A recipient's name and Medicaid ID are considered PHI.

Who decides if I am a business associate? Under the rules, you are a business associate as defined by law; signing a contract does not define your status. Ultimately, the U.S. Department of Health and Human Services gets to decide.

Am I a business associate of Medicaid? If you are a provider for Medicaid but are NOT a medical provider as defined by Social Security (42 USC 1395X(s)) and you receive, create, or maintain PHI on behalf of a Medicaid recipient, you are a business associate of Medicaid.

Why am I being asked to sign this form? The Business Associate Addendum requires you to follow some of the same rules that Medicaid does to protect confidential information. It is required by HIPAA that Medicaid secure this written agreement, which is "satisfactory assurance" that you will "appropriately safeguard" PHI that Medicaid discloses to you.

What do I have to do to comply? There are many components to HIPAA compliance. The list below is an overview. Addressing requirements depends on a variety of factors such as the form of the PHI and the nature of the services you are providing. We strongly urge you to understand your compliance obligations under HIPAA. See the Office for Civil Rights website at http://www.hhs.gov/ocr/privacy/index.html

Business associates must:

• Not use or further disclose the PHI other than as permitted or required by the agreement or as required by law.

• Agree to comply with the policies and procedures and documentation requirements of the HIPAA Security Rule.

• Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the agreement.

• Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI.

• Report any unauthorized use or disclosure of the PHI to the Covered Entity.

• Report any security incident to the Covered Entity.

• Return or destroy all PHI at the termination of the agreement, or, if return or destruction is not feasible, you must continue to protect the PHI even after termination.

• 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.

• 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.

• 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.

• 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.

What if I don't comply? A business associate is directly liable under the HIPAA Rules and subject to civil and criminal penalties for uses and disclosures of protected health information that are not authorized by its contract or required by law.

Why can't you do this for me? No one but you has the authority to mandate and enforce your policies and procedures. It is not possible for anyone else to assemble your policies and procedures without knowing your process of data collection and workflow. Only you and your staff truly know how your business runs on a daily basis. HIPAA compliance is an ongoing process to protect your business and patient's privacy.