Who Is Your Business Associate?

The purpose of this article is to clarify who is and who is not your business associate (BA). We are all in agreement concerning the importance of protecting PHI when we share it with other parties—one such party is your Business Associate.

When you assign a service to be performed by another person or agency on your behalf, and it involves the use or disclosure of PHI, you are entering into a contract that allows you to share the PHI with said party. This contract is referred to as a Business Associate Agreement or BAA and the other party then becomes your business associate. The BAA spells out the duties the party will perform as well as what steps the BA will take to protect the PHI. The primary focus and purpose of the BAA is to provide "assurances" from the party that they will in fact protect the PHI they use or disclose on your behalf. So, who is your Business Associate? This question can still cause some confusion, but if you apply this two-part test, you can quickly make the determination.

A party is your Business Associate if:

1. The party creates, maintains, receives, or transmits PHI on behalf of the Covered Entity.
2. The party is not a member of the Covered Entities Workforce.

Let's look at some examples of Business Associates while using the CMRT test:

Creates: Utilization review, quality assurance, practice management, and claims processing.
Maintains: Vendors who offer personal health records on behalf of the covered entity or cloud storage providers.
Receives: A CPA firm whose accounting services to a health care provider involve access to protected health information.
Transmits: An independent medical transcriptionist that provides transcription services to a physician.

Remember that if a party is to qualify for the Business Associate title, they cannot be a part of the Covered Entities Workforce.

The following are examples where a Business Associate Agreement is *not* required because the parties involved are not Business Associates:

1. A clinic is not required to have a BAA with a laboratory as a condition of disclosing PHI for treatment of an individual. This disclosure would fall under Treatment, Payment, and Healthcare Operations (TPO) and is permissible.
2. A clinic is not required to have a BAA with the specialist to whom the clinic refers the patient to and transmits the patient's medical chart for treatment purposes. This disclosure would fall under TPO as well and is permissible.
3. A clinic is not required to have a BAA with a person or organization that acts as a conduit for the PHI. For example, the US Postal Service, private couriers such as Fed-Ex, and UPS, and electronic equivalents including internet service providers. Each of these falls under the "conduit exception" of the rule. Conduits serve to move the PHI from point A to point B, do not access the PHI, and any storage is transient in nature and not persistent. However, a cloud fax provider or an email provider would be considered a Business Associate as the storage of the ePHI is persistent and can be accessed.
4. An individual whose functions or services do not involve the use or disclosure of protected health information but contact with protected health information could still occur accidentally. This includes janitorial services or electricians—they may come across PHI by accident, but not as part of their day to day work and so a BAA is not necessary.

The following are examples of relationships where a BAA could be required:

Accrediting/Licensing Agencies (e.g. TJC)	Accounting Consultants/Vendors
Actuarial Consultants/Vendors	Attorneys/Legal Counsel
Auditors	Benchmarking Organizations
Benefit Management Organizations	Claims Processing/Clearinghouse Agency Contracts
Coding Vendor Contracts	Collection Agency Contracts
Computer Hardware Contracts	Computer Software Contracts
Consultants/Consulting Firms	Cloud Service Providers
Data Transmission Providers (PHI involved)	E-prescribing Gateway

Continued on Pg. 2…

Who is Your Business Associate continued…

Emergency Physician Services Contracts	Health Information Organizations
Interpreter Services Contracts	IT/IS Vendors
Legal Services Contracts	Medical Staff Credentialing Software Contracts
Pathology Services Contracts	Paper Recycling Contracts
Patient Satisfaction Survey Contracts	Physician Billing Services
Physician Contracts (non-employed providers)	Practice Management Consultants/Vendors
Professional Services Contracts	Quality Assurance Consultants/Vendors
Radiology Services Contracts	Record Storage Vendors
Release of Information Service Vendor Contracts	Risk Management Consulting Vendor Contracts
Telemedicine Program Contracts	Transcription Vendor Contracts
Telemedicine Program Contracts	Waste Disposal Contracts (e.g. Hauling, Shredding)

In summary, a Business Associate needs to meet two main requirements; first, they must create, maintain, receive, or transmit ePHI on behalf of the Covered Entity and they cannot be a member of the Covered Entity's Workforce. Take a moment today to review your contractual relationships and determine if you have Business Associate relationships that require a Business Associate Agreement. And finally, remember that HIPAA compliance is a journey, not a destination. Happy Trekking.

Hernan Serrano
HIPAAtrek
hernan@hipaatrek.com