Health Information Compliance Alert

SECURITY: KNOW WHAT CONTRACT BEST PROTECTS YOUR PHI

When do TPAs fit better than BAAs? The answer may surprise you

A business associate agreement (BAA) alone might not be enough to safeguard protected health data in all your organization's transactions with vendors and trading partners.

There are situations that may require several contract types to thoroughly protect your patients' health information.

Trading partner or confidentiality agreements may serve your purpose more closely than a BAA does, says **David Szabo**, an attorney with McClennen Nutter & Fish in Boston.

Examine Each Contract Type

Your first step in choosing the agreement that best suits your needs is to understand the differences between the contract types. Here's the breakdown:

Business associate agreements (BAA): The privacy and security rules require that you use BAAs to establish safeguards and other responsibilities business associates (BAs) must provide, says **Mark Eggleston**, the HIPAA compliance program manager for Health Partners of Philadelphia.

Use a BAA when a person or organization performs a service for you that you would normally do in-house. Key: That service must involve patients' PHI.

For example, a service that handles your billing is a business associate because they 1) handle patients' information and 2) perform the service on your behalf. On the other hand, an independent maintenance worker is not a business associate because she neither performs a service that you would normally do for yourself nor comes into contact with PHI.

Caveat: When you sign a contract--whether it's a business associate agreement or another type of binding agreement--you are responsible for both abiding by that contract's terms and enforcing those terms on the other party, explains **Matthew Rosenbaum,** COO for CPI Directions, a regulatory consulting firm in New York, NY.

Trading partner agreement (TPA): These contracts are permitted--but not required--by the transactions and code sets rule to set up a protocol for you to share electronic data for payment, says **Kirk Nahra**, an attorney with Wiley Rein & Fielding in Washington, DC. These agreements are different from BAAs because they only exist between providers and payers.

For example, you might ask your payers to sign a TPA that outlines how you'll exchange electronic data (e.g., electronic claims) and what security measures you'll implement, Szabo says.

Confidentiality agreement (CA): These agreements protect business secrets--such as financial or operating information--from those outside your organization. A CA is typically used with employees in higher-level positions who might have access to your business information, Szabo notes.

For example, you would ask an external consultant to sign a CA if she is helping you develop a new business or beef up your business plan.

Note: While you can ask each employee to sign a CA to protect customer lists, prices and other business information, a strict confidentiality policy will be easier to implement. Good idea: Ask your employees to sign your confidentiality policy to acknowledge that they understand their obligations, Szabo suggests.

Choose The Best Fit

To avoid automatically choosing the BAA for all business and operational needs, ask yourself these questions to pin down exactly which contract type you need.

Q1: Will this person or company have access to patients' PHI?

Q2: Why does this person or company need access to patients' PHI?

Q3: Will this person or company perform services on my behalf?

Q4: What service will this person or company perform?

Szabo offers these two sample scenarios to help you distinguish between contract types:

Scenario A: You submit electronic claims to a health plan. The health plan will have access to patients' PHI (Q1) in order to correctly process your payment (Q2 and Q4). Each party is acting on its own behalf (Q3).

Because the health plan is not performing a service that you would normally perform for yourself and because you are exchanging electronic data, you are permitted (not required) to ask the health plan to sign a TPA.

Scenario B: Your health plan asks you to perform a special quality assurance analysis (Q2 and Q4). You have access to the plan's patient PHI (Q1) and are performing the service on behalf of the health plan (Q3).

Because you are performing a service the health plan would normally do for itself and because you have access to PHI, you must enter into a BAA with the health plan. Important: You may still ask that the health plan sign a TPA if you'll be exchanging electronic data, Szabo stresses.

The Bottom Line

By signing the contract that most closely matches your business need, you'll save valuable resources and ensure that no PHI is inappropriately exposed, Rosenbaum says.