Health Information Compliance Alert

Compliance Strategies: How to Help Your Business Associates Protect PHI

Remember: You don't have to police your associates.

You don't have to bend over backwards to ensure your business associates (BAs) aren't mucking up their privacy and security rule compliance -- or exposing your patients' confidential information.

"As long as you have an agreement with your associates that contains all the requirements of the privacy and security rules, you don't have to monitor" their compliance, assures **Patricia Markus**, a partner with Smith Moore in Raleigh, NC.

But you do have two obligations, notes **Robert Markette**, an attorney with Gilliland & Caudill in Indianapolis. "You have to terminate the contract if the associate doesn't abide by it and you must report privacy or security rule violations" to the secretary of Health and Human Services.

This doesn't mean you can't help your BAs develop strong measures that will protect patients' PHI. Even if the BA refuses to comply 100 percent with your policies and procedures, giving them a copy of the P&Ps helps them see exactly what steps you're taking, Markus assures.

Problem: This will only work with small- to medium-sized associates, asserts **David Patino**, clinic manager with New Jersey's Physical Therapy Services of Morristown. Larger entities like WebMD that are working with countless providers aren't going to change their compliance program to match yours, he adds.

Solution: You can rest easy when it comes to large business associates. Due to the volume of PHI they deal with, they know that any violations could cripple their business, Patino notes. That means they'll be working overtime to protect all the information they receive.

And, you don't have to throw your hands up at any smaller BAs who balk at your attempts to help them structure their privacy or security rule compliance. Instead, ask to see their P&Ps and note what measures they will implement, Markus advises.

Define Your Terms Concisely

Your BAs have to report any security incidents or other violations they uncover, but unless you're working from the same definitions, you could find yourself in some hot water, Markette warns.

Planning: "You'd be foolish not to include the definition of 'security incident' from the rule in your security business associate agreements," Markette assures. That's because a narrower definition could omit crucial details and keep you in the dark about violations.

Rather than allow BAs to define security incidents, give them the freedom to act on security incidents in a way that's reasonable for their organization's size, scope and sophistication.

But you should determine what type of security activity is reported back to you. For example, you probably don't want to know each time another system sends out a feeler to your BA's firewall, but you will want to know if an account is successfully breached.

Important: "You should define exactly what the incident report entails," including how soon you will receive a report after a security incident is detected, Markette stresses. To prevent future disputes, be sure you both agree on a

reasonable timeframe and other requirements before you sign the BA agreement.

The Bottom Line

Your BAs want to do business with you -- and they don't want to be the guilty party when it comes to a security or privacy breach. Your first step in the process is to negotiate a contract you are both happy with.