Health Information Compliance Alert

Privacy: Is Your PHI Swimming In Foreign Waters?

Ensure the security of your outsourced PHI with these suggestions

Is your patients' PHI safe with your business associates? If your BAs are outsourcing to offshore subcontractors, that answer is 'No.' But there's good news: You can take reasonable steps to control where your PHI winds up.

Test The Waters

Start by weighing your risks against the potential benefits, says **Gwen Hughes**, Director of e-HIM Consulting Services at Care Communications in Chicago. Tip: "Talk about your concerns and discuss how you can best protect PHI while it's resting or being transmitted," she suggests.

Problem: While the surface risk may seem slight, don't forget to consider the ripple effect, Hughes stresses. Any bad publicity drummed up by your organization's failure to adequately protect patient information could have disastrous effects.

"Patients could lose faith in your ability to protect their health information. You could lose donations to your foundations. You might lose a valuable third-party contract. And, depending on the size of the breach, you could lose your accreditation," Hughes warns.

Solution: Work with your attorney to find ways to limit risks, experts say. "Make your business associate adhere to the laws of the U.S. and demand that they put everyone through HIPAA training and that litigation will happen in the U.S.," Hughes asserts.

Strategy: Use indemnity to force business associate accountability for your patients' PHI, experts stress. "While the contractor can't take the bullet for you on a HIPAA violation with HHS' Office for Civil Rights, they certainly can be financially responsible for a violation" if there is a state privacy right of action, assures **Clark Stanton**, an attorney with Davis Wright Tremaine in San Francisco.

Know Your PHI Stream

Currently, about 20 percent of medical transcription work goes to India. When a Pakistani transcriptionist blackmailed the University of California-San Francisco in November 2003, the risks associated with offshored PHI flew onto everyone's radar screen.

As a result, providers have no excuse for not being aware of it and taking steps to prevent privacy breaches, Stanton says.

How do you do that? Many entities have decided to stop sending their PHI offshore, explains **Jason Levine**, a consultant at Joliet, IL's Murer Consultants. This requires providers to really inspect where and how their PHI is subcontracted, experts say.

"If you're going to outsource, you need to know from the people with whom you are outsourcing where the information is actually going," Stanton emphasizes. You can easily "require them to notify you and get your authorization before sending PHI" to a subcontractor outside of U.S. jurisdiction, he adds.

Take The Plunge

If you are willing to take the risks involved with offshoring your patients' private health information, there are some things you can do to lessen your chances of a HIPAA violation.

Ask around. "If you must outsource your PHI, then you need to make sure that the company is reputable," Hughes says. If they've worked with you before, you know their track record and you can better control the relationship, she says.

Also, you can use "highly regarded sources like AHIMA's vendor directories and your colleagues," she suggests. Ask questions about the contractor's quality
and turnaround, their HIPAA training process and how comfortable providers are with that contractor's services, Hughes offers.

Use the BAA. The business associate agreement (BAA) is crucial to avoiding HIPAA violations down stream because it sets up what you will and will not tolerate from your business associate, explains **William Hubbartt**, president of Hubbartt & Associates in St. Charles, IL. "Use the BAA to guide what requirements the business associate must fulfill to protect privacy," he clarifies.

The BAA is an agreement that sets out the definitions and requirements of the business associates' services, Hubbartt reminds.

Strategy: "You can force them to implement certain privacy and security practices, including an audit to make sure they aren't wrongly disclosing information," he asserts.

Tip: Demand that the business associate "establish its own procedures that allows access to PHI, including the ability to file a complaint and request an accounting of disclosures," Hubbartt suggests. Applying the obligations of the covered entity to the business associate will make them less likely to put your PHI in a risky situation, experts agree.

Come Up For Air

"Your business associate should inform you of any privacy breaches," but they may not, Hughes cautions. Often, PHI is subcontracted to areas where the privacy laws aren't as strict as ours, she reminds. They could be misusing your information and not even know.

"You have to let people know if their information has been compromised and you have to report breaches to the Department of Health and Human Services," Levine advises. And, honesty is the best policy, Hughes counsels.

"Tell your patients that you failed to protect their information and then tell them what you're going to do about it," she suggests. Letting them know how much damage has been done and what steps you are taking to fix it could help you avoid a lawsuit, she contends.

The Bottom Line: "It's a matter of trust," Hughes explains. Being up front with your patients and being willing to help them through the fall out will endear them to you and may keep you from losing a valuable customer, she reminds.