Health Information Compliance Alert

Compliance Strategies: Have You Hit The PHI River Without A Paddle?

Avoid rough waters with a business associate agreement.

Do you store your PHI at a data warehouse? If your answer is "Yes," then you'd better grab a business associate agreement (BAA) before your PHI ship is sunk.

Get The Right PHI Flow

Keep in mind that not all warehoused data is the same. "You only need a business associate agreement with your vendor if they are getting PHI," explains attorney **Michael Roach** at **Chicago's Michael C. Roach & Associates**. If the data sent to the warehouse is deidentified, then there is no obligation to obtain the agreement, he confirms.

Encrypted PHI is trickier, experts agree. "An encrypted file in its native form can't be read and isn't PHI," states Marc Goldstone, an attorney with Hoagland Longo in New Brunswick, NJ. Warning: "Encrypted PHI can be decoded" and people can easily get into your patients' files if you don't use a strong encryption method, he warns.

Consider these scenarios:

Scenario A: You hire a third party to strip your patient files of all identifiable information and they then send those files to a warehouse.

Scenario B: You bundle medical records and send them to the warehouse. All the warehouse knows is that it has Bundle 1. When you need particular records, you call the warehouse and ask them to send you Bundle 1.

Scenario C: You send the warehouse all your patient files and they bundle them. When you want a particular record, you call the warehouse and ask for it by name. The warehouse goes into the bundle and pulls that record.

In Scenario A, there is no way for your patient's information to be used inappropriately, so you do not have to sign a BAA with the warehouse. However, "very rarely is there a reason to warehouse deidentified data," Goldstone says. While the third party deidentifier is a business associate, you probably don't need to spend your time and money on a warehouser.

Scenarios B and C up the ante. Scenario B puts the warehouser in the position of a conduit, Roach posits. "We know that couriers like the post office are not business associates," he says. The warehouse is simply moving the bundles, not accessing or using the information within.

In Scenario C, the warehouse not only handles your patients' files, it has full access to the information contained within them. That means patients' private health information is vulnerable. A BAA will force the warehouser to protect that sensitive information from a privacy or security breach, experts remind.

Here's How to Play it Safe

Whether you bundle (encrypt) the files you send your warehouser or you ask them to do that for you, a BAA could keep you dry in the middle of a **U.S. Department of Health & Human Services** (HHS) storm.

Tip: If you're hesitant about entering into yet another BAA, "a confidentiality agreement will provide many of the same protections as the BAA," Goldstone offers. And it could save you from the hassle and bad press of any HHS involvement.

Most important: You must know if there is a breach at the warehouse, Goldstone stresses. If too many problems occur, you may need to "find a new data warehouser, do some remediation, and possibly notify your patients," he explains.

Remember: You're the one at risk for a HIPAA violation, Roach reminds. A business associate or confidentiality agreement will prove that you made a good faith effort to protect patients' information at all stops down the road.

Failure to force the warehouser into an agreement won't sit well with regulatory authorities. If HHS "thinks you're playing fast and loose with the law, they could turn a violation over to the Department of Justice," Roach warns.