Health Information Compliance Alert

Security Strategies: 4 Tips To Buttress Your Backup Process

Strengthen your plan before you get backed into a regulatory corner.

Worried that your backup plan is full of holes? Our experts share the following four tips for shoring up your data storage process.

1: Study Your State

"Every state has its own retention laws," warns attorney **Beth Rubin** with **Dechert** in Philadelphia. You must keep records for a determined length of time, but there is no mandate on how you keep them.

"You can store them offsite with a storage company or image all your records and archive them," Rubin suggests. **Key:** As with all of HIPAA's requirements, you must do only what is reasonable for your facility's size and scope. If imaging is too costly and burdensome, it may not be an option for you, Rubin suggests.

2: Get Physical

Physical security must be a top priority in your backup plan, insists **Raj Patel,** manager of **Plante & Moran's** Security Assurance and Consulting Practice in Southfield, MI. "You don't want someone to walk in and grab your tapes," he explains.

Physical security will also protect your backups from fire, wear and tear and temperature damage, he says. Patel suggests that you store your data in a lock box or other fireproof container.

If you decide to depend on an external site to store data for you, make sure you transport the PHI in a safe environment, Patel cautions.

Tip: "Don't take your data in the car with you while you run your errands" or leave it in extreme temperatures, he warns.

And you must ensure that whoever you contract to help with your backup plan signs a business associate agreement (BAA). The agreement should say that the "company will segregate your tapes from other clients," Patel counsels.

3: Double Up

A strong physical security procedure could be enough to keep your data from unauthorized use and disclosure, but in order to be fully confident, you need to add one more layer -- encryption, Patel says.

"Some backup systems will encrypt the data as it is recorded, or you can buy a second application," Patel states. While this process adds one more step and could slow down your process, it strengthens your plan. "Even if the data is compromised, [unauthorized viewers] will have a hard time reading it," he explains.

The second layer of security could slide your compliance effort into due diligence. If a violation does occur, your policies will show how hard you worked to avoid such compromises.

4: Be Realistic

HIPAA demands that you have a written policy and procedure for your backup plan.

Caution: "Only write policies about what you're going to do -- not what you think you should do," Rubin stresses. "It's

worse to have a policy you can't live up to than not to have a policy at all," she adds.

And if you document how you developed your backup procedure, it will be difficult to second-guess your decision later on. "There's no guarantee your policies and procedures won't lead to liability, but you will be in a much better position to justify your decisions," Rubin says.