Health Information Compliance Alert

SECURITY: DON'T AXE THE SECURITY RULE'S ADDRESSABLE STANDARDS

Instead, whittle them down to fit your needs

You can't ignore the security rule's addressable standards, but you can pick and choose the ones that work best for your organization. The best part? Applying a standard in one area doesn't obligate you to use it across the board, experts tell **Eli**.

CUSTOM CARVING

Each covered entity has to look at the addressable standards and decide "whether and how they would be appropriate," says **Robyn Meinhardt**, an attorney with Foley & Lardner in Denver, CO. The standards are addressable because not all of them are appropriate for some organizations, she reminds.

So where do you start? "The decision is based partly on your risk assessment and partly on feasibility," explains consultant **Jason Levine** with Murer Consultants in Joliet, IL. "You've also got to consider what kind of grief [the standard] is going to cause" for your end users, he warns.

Don't forget to weigh all the factors, cautions **Patricia Markus**, a partner with Smith Moore in Raleigh, NC.

Some determinants include:
Facility size
Number of users
Resources
Current programs
Budget

"Start with a needs assessment and ask, 'Who are my stakeholders?'" suggests **Kathy LePar**, a senior consultant with Beacon Partners in Norwell, MA. Knowing who will be affected by your choices -- and what their needs are -- will allow you to make better decisions about which standards fit best, she says.

Tip: "Make a dream list," LePar advises. Your list should be built from the needs of each department without taking into account any budget restrictions. Once the list is compiled, filter and sort the items until you arrive at a compliance picture that is customized by department, she counsels.

Remember: You don't have to apply addressable standards across the board, Meinhardt says. "What works in the ER won't necessarily work for the home health agency," she explains.

LEAVE YOUR MARK

The key to applying -- or deciding against -- an addressable implementation specification is documentation. If you choose not to adopt a certain standard, "you still have to implement an equivalent and document how you are nonetheless meeting the standard," Meinhardt affirms.

If your organization is small, you won't need as much paperwork, experts agree. If you have a large office with lots of risk, you "must go into detail about why [the addressable standard] is not reasonable and appropriate for you," Meinhardt declares.

The good news? "It's unlikely that you'll see the Office for Civil Rights second guessing your reasoning," Levine states. If your documentation proves that your compliance program is reasonable, "then you're pretty safe," he claims.

Tip: Work with your lawyers along with any security consultants, Markus advises. That way you can attach attorney-client privilege to all your documentation. If there's ever a security breach, that information can be better controlled, she says.

THE BOTTOM LINE

No matter what you implement, your main focus must be on integrating that standard into your culture.

Technology is only 10 to 15 percent of the solution, LePar reminds. The other 85 percent comes from your people and your operations.

Tell your employees why you're choosing a certain standard -- and how they'll benefit from that choice, LePar recommends. In doing so, you'll bring them on board. Without employee buy-in, "HIPAA compliance is an uphill battle," she adds.