Health Information Compliance Alert

Security: 3 Strategies That Will Help You Gauge Your Security Risks

Whether you're a large or small provider, time is running out

If you haven't started combing through your office's security risks, you are setting yourself up for a security rule violation. Here's some expert advice to help you get started.

Take A Mental Snapshot

The security rule doesn't give you a "cookbook recipe" for performing a security risk assessment, says **Rick Ensenbach**, Senior Security Consultant for **Shavlick Technologies** in Roseville, MN. So, what should you do first? Take a mental snapshot of where you are right now and note the risks your present activities pose when viewed against your potential threats, Ensenbach says.

Next step: Make an actual checklist that ranks your risks from low to high, advises **William Hubbartt** of St. Charles, IL's **Hubbartt & Associates**. Once you've taken the snapshot and made the checklist, you will have a laundry list of information that tells you exactly which areas you need to focus on first -- and which are already secure.

Prove To CMS You're Doing Something

When it comes to the rule's addressable (general rather than specific requirement) implementations, you have some options. You can:

1. Check to see if you are already in full compliance, based on your risk assessment.

2. Create a compliance plan and budget, get executive approval and move forward on your plan.

3. Implement a control that is reasonable for your office's size and scope, but one that can accomplish the same goal.

4. Take no action and explain why you cannot comply. Then note -- and document -- what you will do instead to ensure protection of your patients' PHI. **Important:** A senior manager must sign off on this. (**Hint:** This option will be the trickiest one to sell to CMS).

Remember: No matter what choice you make, you have to document your decision-making process and rationale. Your documentation will provide a safety net to prevent compliance hassles down the road, experts concur.

For example, you need to send PHI in an unencrypted email to another doctor, but you're worried that this may be a violation of the security rule, which says you must take "reasonable and appropriate security measures to protect PHI from unauthorized access," Ensenbach affirms.

If the doctor you plan to email is within your computer network (internal), interception by an unauthorized person is unlikely, so your encryption need and security risk is probably low. On the other hand, if you send email outside your network (externally), especially over the Internet, then the encryption need is high, Ensenbach advises.

Here's Ensenbach's example of your options for acting on this addressable requirement:

1. Encrypt all outgoing email or choose to stop sending PHI over email outside of the organization. Both methods show your compliance.

2. Fax the PHI rather than encrypt the email with PHI. This would count as a "mitigating" (reducing the risk) control, but

you'd better show that you added the following safeguards:

a. Called the receiving party just before sending the fax;

b. Stood by the fax during its transmission;

c. Arranged for the other person to stand by the fax; and

d. Called to confirm immediate physical receipt and removal of the fax.

3. Send outgoing email without encryption and hope that nothing compromises your patients' PHI. **Important**: Keep yourself out of the hot seat by getting senior management's sign-off, but remember that this still represents a significant risk for your organization's reputation, suggests Ensenbach.

Know Your Boundaries

The security rule says compliance does not have to break your budget or your back. That means you're in good shape if you make an appropriate "business choice," says **Susan Miller**, a healthcare consultant in Boston. The rule's requirements are "scalable, flexible and technologically neutral." This means you can match technology -- and security measures -- to your office's specific needs, budget and physical circumstances.

Keep in mind: Technology decisions are complex and can be very expensive. Although you don't have to choose the most current and upscale software programs with high-level internal security controls, sticking with outdated programs that are hard to secure will block your compliance efforts, counsels Miller. And if you aren't confident you can perform an adequate risk assessment and implement the necessary changes, don't hesitate to ask for help from a qualified professional, Ensenbach adds.