Health Information Compliance Alert

SECURITY ~ 12 Steps To Security Compliance Success

Hint: A careful risk analysis can put you back on track.

How secure is your protected health information? If you're not sure, it's definitely time to recheck your policies and implement new ones if need be.

Take a look at these tips to make your policy and procedure planning go a bit easier:

1. Let Common Sense Prevail, Not Technology. "Ninety percent of security is what's between people's ears, not necessarily what technology they implement," says **Tom Hanks,** National Director of HIPAA Practice for **PricewaterhouseCoopers.** You're already familiar with the dos and don'ts of privacy rule compliance. That's more help than you probably realize when you're implementing your security rule plan.

2. Focus On Three Areas Of Compliance. Administrative, physical and technical safeguards: Those are the three areas the **Department of Health and Human Services** wants CEs to be familiar with.

Remember that the security rule is technology-neutral, and you can choose almost whatever policies and procedures will work for your organization. HHS realizes that a two-person physician practice has different needs than a large hospital, for example.

3. Risk Analysis/ Management A Must. This is the key to your security rule compliance plan, says **Bill Braithwaite,** National Director of HIPAA Advisory Services for PricewaterhouseCoopers. That means compiling an accurate assessment of potential risks and vulnerabilities within your organization.

Run a risk analysis to determine what those vulnerabilities are, advises Braithwaite, and then ensure you have the appropriate sanctions in place against workforce members who fail to comply with your policies and procedures.

Important: As one of its implementation specifications, the security rule requires an "information review system," which means not just keeping audit logs, access reports and incident tracking reports, but reviewing them. "It's absolutely no use to have the logs if you don't review them," Braithwaite notes.

And others agree that the risk analysis is the most important first step CEs can take. **Michael Roach,** an attorney with the Chicago office of **Michael, Best & Friedrich,** tells **Eli** he performed a risk assessment for a client recently. "I walked through a client's facility and afterwards said, 'I see CDs sitting around cubicles and nobody's sitting there. Do you have a policy where people who aren't employees can, because they may have a badge on them, roam through this workspace unattended?'"

Roach says in order to know the items you'll need to address, you must know the current state of your security systems. Once you've done that, he recommends that CEs create a checklist from the security rules, a tool that should obviate a haphazard approach to compliance. "That way, you can make sure that your program is addressing everything that's required," he notes.

4. Assign Security Responsibility. This means a person, not a committee, Braithwaite warns. It sounds simple, but someone has to have the responsibility of developing and implementing your policies and procedures that make your security plan work.

5. Ensure Workforce Security. You have to ensure that the members of your workforce have appropriate access to

protected health information, urges Braithwaite. "Appropriate access" means you'll have to consider whether or not you'll need to have procedures in place to authorize and supervise workforce members that have or could have access to electronic PHI. This also applies to employees who've been terminated; they'll have to be cut off from access to PHI when their employment ends.

6. Train Your Staff. The security rule specifies that all staff members must have security principles training. Braithwaite advises CEs to perform periodic security updates, say, via a group email or a newsletter. "Remind your workforce what they should be doing in terms of their security procedures every so often," he says.

Good idea: Implement protections from potentially malicious software out there. Additionally, the person responsible for your security plan should monitor login attempts and manage passwords, he urges.

7. Report Security Incidents. Part of your policies and procedures should include addressing security incidents when they occur. That means having a response mechanism and then reporting those incidents. Identifying and responding to such incidents effectively and efficiently will help you to mitigate possibly harmful effects.

And, if you do have a security breach, make sure to document it and its outcome, says Braithwaite. That way, you'll be able to show exactly what happened and, more importantly, what you did to prevent it from recurring.

8. Have A Contingency Plan. Responding to an emergency situation is critical for any CE. Data backup and disaster recovery plans and emergency mode operation plans are required. What happens, for example, if your computer system is on the blink and you still have to treat patients?

Testing and revising your contingency plan and procedures in emergency situations is especially important for larger organizations, says Braithwaite. Whatever your contingency plan looks like, it's important for you to analyze what are the most critical things to keep going when an emergency occurs.

9. Update/Review Your Policies And Procedures. The rule requires you to perform a technical and non-technical evaluation of your security plan to establish whether or not you're meeting the rule's requirements.

While "periodic" isn't defined, Braithwaite says, "Every year or two is a good rule of thumb." But remember that software updates can occur more frequently, and he says whenever a vendor updates your software or replaces your old system with a more recent version, that's the perfect time to run an evaluation to ensure your policies and procedures are still up to snuff.

10. Review Your BA Agreements. Roach says this is extremely important. Odds are you already have your business associate agreements in place that focus on the privacy rule. Unfortunately, the additional security rules mean you'll have to tweak those agreements to conform with some of the security regs, he cautions.

Once you've got a BA agreement for privacy, the additional language for security is fairly minor, Roach states. While it shouldn't cause you undue frustration, it's important to get it done ASAP, he warns

11. Review Your Facility's Access Controls. A "facility" is really anywhere where electronic data is stored. Ask yourself this: Can anyone at all waltz into your computer room and make changes to a file?

Think about all of the areas in your organization where someone could walk up to a workstation and make changes, advises **Cynthia Smith,** Senior Manager with PricewaterhouseCoopers. You know more than anyone else what's best for your organization, and you'll be obliged to come up with appropriate access controls based on your specific needs.

Strategy: You'll have to come up with access controls for laptops or PDAs, for example. If a laptop that's been taken home for the day is stolen, you'll need to ensure that even though the computer is missing, patients' PHI is safe through encryption controls.

The security rule isn't specific on these physical safeguards mainly because they should be specifically tailored to fit your

needs.

12. Keep Maintenance Records. If there's an accident or a situation that adversely affects your system, it could be that a line was accidentally cut. Or maybe there was a phone switch change.

Whatever the case, keeping and maintaining maintenance records could help you identify not only who might have made the mistake, but also where you can focus your efforts to get the system back up ASAP.