Health Information Compliance Alert

Security: 5 STEPS TO GUARANTEE YOUR SECURITY MEASURES MAKE THE GRADE

Professional guidance will ensure your security rule compliance - before it's too late

The security rule compliance countdown has begun. The bad news: You have fewer than six months to pass your toughest compliance test yet. The good news: HIPAA security experts divulge to **Eli** five key steps that'll help get your security program in tip-top shape.

1. Create your compliance team.

Security compliance isn't a one-man job, explains **Beth Rubin**, an attorney with Dechert in Philadelphia. When creating your team, use a multidisciplinary approach, Rubin recommends. That means you should bring in employees from across the organization - IT staff, compliance professionals, legal experts and other key players.

Tip: Identify one person to lead your team, preferably your security officer, suggests **Greg Young**, security officer for Mammoth Hospital in Mammoth Lake, CA. "Somebody has to be in charge of your compliance efforts to ensure nothing is missed," he notes.

"The first 30 minutes of your team's initial meeting should be dedicated to educating members on the [security] rule," Rubin stresses. Good idea: Send team members an information packet or security rule 'cheat sheet' ahead of time, she proposes.

2. Develop a task-specific action plan.

The result of your first team meeting must be a decisive action plan that outlines how your organization will tackle its security rule compliance, Rubin says. "That includes a strict timetable for when each task will be completed," she adds.

Rubin recommends your action plan answer the following questions:

1. Who will conduct the risk assessment?
2. When will the risk assessment be completed?
3. Who will be in charge of risk management?
4. Who will review business associate agreements?
5. When will all agreements be finalized?
6. Who will draft and review policies and procedures (P&Ps)?
7. When will training begin?

Be sure that each member of your team has a copy of the action plan and that they meet frequently over the next few months. Remember: Your team must be accountable to the action plan to meet the compliance deadline, Rubin asserts.

3. Assess and manage your organization's risks.

"This is the heart of HIPAA's security rule," Rubin assures. But it doesn't have to be a huge ordeal, says security consultant **Chuck Connell** of www.HIPAASecurityExperts.com. Tip: "Focus on the standards first," he suggests.

Once you pin those down, you can attack the addressable implementation specifications, Connell says. (See HICA Vol. 3, No. 5 for more information on required versus addressable implementation specifications.)

Best approach: Use your risk assessment to guide your risk management process. "Highlight the highest risk areas in your organization and fix those immediately," Connell suggests. Once those issues are under control, you can address the rest.

Keep in mind: Conducting a risk assessment is the most time consuming step, Rubin acknowledges. You should allot the most time to accomplish it, she says.

4. Fine-tune your business associate agreements.

You don't have to renegotiate all of your business associate agreements (BAAs), but you may need to add an amendment to those agreements that outlines your organization's security plan, advises Rubin.

Caution: Update your agreements pronto, Rubin warns. Otherwise, you could wind up at the mercy of your business associates. "Many vendors are planning to send out a one-page agreement at the last minute and that will put them in the [security compliance] driver's seat," she says.

Better idea: "Send out the language you prefer and use the security rule amendment as an opportunity to take control of your relationships with your business associates," Rubin counsels.

5. Write and implement your policies.

After you've done the risk-assessment heavy lifting, writing out the procedures your staff will use to comply with the rule will be easy, experts say. Tip: Choose one person to write all your P&Ps, Young suggests. That way, you'll ensure consistency - and any conflicting measures can be resolved quickly, he says.

Next step: Train your employees on your organization's compliance plan. You don't have to wait until the end of the process to do that - start by teaching them basic security controls and then focus your training as your P&Ps develop, Connell suggests.

The Bottom Line: "You've got some major work to do to be ready by April 20, but it is doable" Rubin says. And even if you aren't completely finished with your compliance efforts by the deadline, you are in a better position to avoid a violation if you can show that you are doing your best.