Optometry Coding & Billing Alert

Clip and Save: Get Hip to HIPAA Before It's Too Late

Prepare your optometry practice for this month's security rule deadline

Is your optometry office ready to meet the April 20 deadline for compliance with the Health Insurance Portability and Accountability Act's security rule? If you're like 82 percent of surveyed physicians, you're not. But don't panic - there's still time.

The Healthcare Information and Management Systems Society and Phoenix Health Systems sponsored a February survey that found 18 percent of healthcare providers who responded were compliant with the HIPAA security regulations.

The biggest roadblocks: Overall integration of new systems, policies and procedures is the biggest challenge, with interpretation of HIPAA regulations and budget and time constraints following behind, the survey results said.

You still have time to get in compliance if you start right away and tackle the requirements head on, experts say. Even if you aren't in full compliance by April 20, you should show that you have a specific plan to get in compliance - including a finish date - and that you are well on your way to completion, says **Misty Maw,** practice administrator for Professional Eye Care in Canton, Miss. This proof can work greatly in your favor if you find yourself on the business end of a HIPAA enforcement action.

Save This Checklist to Verify Compliance

Use the following checklist, created by **John Parmigiani**, senior VP for Consulting Services at QuickCompliance in Avon, Conn., to measure where you are - and how far you have left to go - in the process.

Remember: Even if you think your security rule compliance is in the bag, "it is a good idea to have an independent validation of your security compliance efforts," Parmigiani says.

-Have you designated someone as a security officer and defined the duties?

-Do you have a security management process in place?

-Have you reviewed your information security policies and procedures? Do they address all of the HIPAA security standards?

-Have you performed a risk analysis of your organization - identified all of your information assets, their vulnerabilities, your "threat profile" and assessed the risk impact?

-Have you created a security training program for all of your staff that is both general for everyone but also focused for those specific functions that carry out your daily business responsibilities?

-Have you created a risk management plan that enables not only regulatory compliance but also viability in an e-health environment?

-Are you confident that your business associates are providing the same level of security for your PHI as you?

-Have you identified your most critical applications and the information that is essential to your office, and have you provided for a business continuity/disaster recovery plan?

-Are your entity's authentication controls adequate to prevent unauthorized access to your systems?

-Do you regularly audit your systems to determine who had access and when, if there were any attempts to exceed authorized access levels, and/or if there were any access attempts by unauthorized users?

-Have you established strong password procedures?

-Will your media, workstation and virus-checking controls measure up to compliance requirements?

-Do you have a process that ensures network security?

-Do you have a process that provides for the physical security of your facility?

-Are systems periodically tested for effectiveness of their security features?