Codify
BY AAPC

Health Information Compliance Alert

Avoid Spending Thousands To Clean Up HIPAA Compliance Issues

Follow these 8 tips to comply with security rule.

How would your practice handle the notification process for a HIPAA breach? Between 2009 and 2011 the **Centers for Medicare & Medicaid Services** had to notify 13,775 Medicare beneficiaries that their privacy had been breached. This likely cost the agency and/or its contractors well into six figures, if not higher, in employee resources, mailing costs, and legal consulting fees.

Even a much smaller breach could put your practice into financial disarray, considering the fact that you'd not only want legal advice, but you'd have to begin the notification process. Luckily, you don't have to spend a fortune to comply with the HIPAA rules up-front, which can save you problems down the line. Consider these eight tips to ensure that you're in step with patient privacy.

1. Ensure that each employee has a separate username and password for your computers. Many physician offices have one username and password for everyone, but you should have separate accounts for each person. Also, if each employee signs in under his or her own name, you can tell who's altered which files. If you're using Microsoft Windows or Mac OS X, you should be able to set up multiple passwords easily.

2. Unplug all modems whenever someone isn't actively using them. This makes it more challenging to hack into your system.

3. Look at what your business associates are doing. If your software vendor comes in regularly to update the software, make sure you know what this person is actually doing in your office and what he has access to while he's there.

4. Don't just buy an off-the-shelf HIPAA solution. If you do, it won't reflect requirements in your state. And tailoring your own solution may be cheaper than adapting someone else's solution.

5. Choose your employees carefully. In a really small practice, with only a few employees, you probably won't set different levels of access to information for different employees. So instead of setting access privileges for each employee, just make sure you hire good and trustworthy people, and evaluate them at the interview stage.

6. Encourage security literacy among your IT staff. Ensure that your staff members are aware of the potential weak areas in an IT system and allow them the training to stay on top of how to close those gaps.

7. Keep an eye out for people wandering around your back office who don't seem to belong there. In a small practice, your staff will know each other -- and maybe all of the patients -- by sight, so they should be able to tell at a glance if someone seems out of place.

8. Put monitors behind a counter or position them so patients can't read them.

CPT® 2023 American Medical Association. All rights reserved.