Codify
BY AAPC

Part B Insider (Multispecialty) Coding Alert

HIPAA: Don't Make A Million-Dollar Mistake On HIPAA Compliance

9 tips to comply with security rule, in effect April 20

Even before the new HIPAA security rule took effect, one physician practice may have been out a million dollars due to lax security compliance.

The **San Jose Medical Group** had to notify 185,000 current and former patients that their private information was compromised. A burglar stole computers containing patient names, addresses, billing information and Social Security numbers from a locked room, according to press reports.

That lapse is "going to cost them about a million dollars," estimates **Clyde Hewitt**, a security consultant with Buffalo, NY-based **CTG**, an information technology consulting firm. The biggest expense won't be Health Insurance Portability and Accountability Act (HIPAA) fines, which can total $100 per violation and a maximum of $25,000 per year. Rather, the highest cost will be notifying all those patients, as California law requires.

Several bills under consideration in Congress also would make it a federal requirement to notify people when their private information gets loose, Hewitt notes.

Security Rule Now In Effect

The HIPAA security rule took effect April 20, and many small physician practices are struggling with compliance. Luckily, you don't have to spend a fortune to comply with the rules. Hewitt and other experts offer these suggestions:

1. Give each employee a separate username and password for your computers. Many physician offices have one username and password for everyone, but you're required to have separate accounts for everyone, says attorney **Robert Markette** with **Gilliland & Caudill** in Indianapolis. 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, says Markette.

2. Unplug all modems whenever someone isn't actively using them, Hewitt advises.

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, Hewitt advises.

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, says attorney **Robyn Ellis** with **Gentry Locke** in Roanoke VA.

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, notes Markette. "For most small providers like that, everyone needs to be able to access everything," he says. 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, says Markette.

6. Encourage security literacy among your IT staff. "You can't secure a 32-bit operating system with a two-bit administrator," Hewitt quips.

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 the patients - by sight, so they should be able to tell at a glance if someone seems out of place, says Markette.

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

9. Read the white paper on "Small Practice Security Implementation" published by the **Workgroup for Electronic Data Interchange** in Reston, VA. The document includes tips on performing a risk analysis and risk management for small physician offices. You can find it online at http://wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/20040420SmallPractice.pdf.