Health Information Compliance Alert

THE THIRD DEGREE: READER QUESTIONS ANSWERED: Got HIPAA Questions? We've Got Answers

From properdisposal of files to the appropriate use of passwords in your workforce, we know there are specific concerns faced by various covered entities throughout the nation. You're asking the tough questions, and thanks to some of our esteemed HIPAA experts, your queries won't fall on deaf ears. Take a look below at what your colleagues need to know.

Question: A Utah subscriber asks: **How should our medical practice dispose of hard copies of files?**

Answer: There's no debate here; shredding is the only answer, says **Megan Hardy**, CMM, office manager with the **Poronsky Family Practice** in Palos Heights, Ill. Hardy advises medical practices to shred anything with patients' names on it. "Depending on the size of your practice," she adds, "you might even need to hire a shredding service. We started doing it in-house, with a couple of shredders of our own, but quickly burned out the shredders from so much use."

If that seems like a lot of trouble, Hardy says appearances don't deceive. "But as horror stories accumulate - from tales of boxed medical files falling out of the beds of pickup trucks to accounts of boxed medical files sitting in parking lots alongside dumpsters, it's clearly the right preventive measure."

Hardy adds that if your shredding service does a lousy job disposing of your documents, you're the one who'll be held accountable. But don't fret, she says. "One way to know what you're paying for is to hire a service that will drive its trucks to your office and shred your documents onsite, while you wait. Make sure your service is HIPAA-compliant, and remember that most of the horror stories involve a low-cost or 'cut-rate'shredding service."

Question: A subscriber in a Chicago hospital asks: **Since the security reg is 'technology-neutral'and doesn't require CEs to buy new software, can we get by with coming up with something on our own? Are we going to get nailed by the feds if there's a security incident and our security plan software isn't viewed as being up to snuff by the feds?**

Answer: Breathe slowly, relax, and let the answer of one of our experts take you into a HIPAA happy place. "There is absolutely nothing in the final security rule that is not already incorporated into the software products that are in common use today," says **Harry Smith**, president of the Denver chapter of the **International Systems Security Association**. Smith does add one exception, however: If you're running Microsoft Windows 95/98/ME, you'll have to upgrade to Windows NT/2000/XP, but he adds that that shouldn't stand in your way.

Smith says many security product vendors will try to sell you expensive solutions, claiming that you won't be compliant without them. "Don't fall for any 'HIPAA hype,'" he warns, adding that there are three aspects of technical security, which he calls the three "As": authentication, access control and audit. Almost every operating system, database system, and patient information system includes built in controls that address the three As.

Most likely, "all you'll have to do is dust off the User's Guide and figure out how to ensure that everyone has his own user account and password, set the appropriate file permissions for sensitive information, and turn on activity logging," he notes.

Question: A subscriber from a Pennsylvania Ob-Gyn Practice asks: **Can we leave phone messages on a patient's answering machine?**

Answer: Yes, but with some caveats, since when it comes to answering machine messages, "less is definitely more," advises **Melissa Cornwell**, HIPAA coordinator for **Floyd Regional Medical Center** in Rome, Ga.

Cornwell advises practices not to leave messages with medical information and notes that making any mention of radiology or biopsies or pap smears is over the line. In fact, she says, "don't leave more of a message than to say, 'Hi, this is so-and-so from doctor so-and-so's office. Please call me at such-and-such a number." The best way to cover your bases is to take a preemptive approach, Cornwell urges. When the patient comes in for his first appointment, have him fill out a form that asks him to specify how you may leave phone messages whether on his machine or with a designated relative.