Codify
BY AAPC

Optometry Coding & Billing Alert

HIPAA Help Desk: Keep Tabs on Floppies and CDs Containing Patient Info

Follow these 6 tips to remain HIPAA-compliant

If you leave the office with portable media such as diskettes, floppy disks, CD-ROMs and portable computers that contain protected health information (PHI), make sure you're HIPAA-compliant or you may have to leave the office for good.

HIPAA, according to the HHS, is designed to "protect medical records and other individually identifiable health information, whether it is on paper, in computers or communicated orally."

While protecting health information shared on paper and in conversation is comparatively simple, safeguarding protected health information on computers and portable media such as disks or PDAs is more complicated, particularly in a small office setting.

Here are six simple rules you can use to keep diskettes, floppy disks, CD-ROMs and other media properly accounted for.

Rule 1: Identify Your Problem Areas. How many diskettes contain PHI in your office? Do you know where they are at all times? You need to address at least two basic types of problems with removable media. On the one hand, you may lack proper controls and, on the other hand, you could encounter malicious copying of media. While experts admit there's not much you can do to prevent the latter, you can still make it more difficult for unauthorized personnel to gain access to media devices.

Rule 2: Limit Placing PHI on Removable Media. This is probably the best solution for media control. And make sure your backup disks are in a safe place. "We use a disk system for backup, and we back up daily," says **L.R. Gabe, OD**, in Show Low, Ariz. "I take them out of the office daily. The disks are taken home to my residence to a small home safe." Even if all you have on disk is billing information, you are still required to safeguard it. "Our patient billing is on computer, and it's backed up on a daily basis onto a CD, and the doctor takes it home with him on a daily basis," says **Terrie Call, CPOA**, office manager at Toler and Toler Optometrists in Richmond, Va.

Rule 3: Store Media in a Safe Zone. Sounds simple enough, but in many cases PHI-containing media devices can get out in the open due to the lack of proper storage, or simply through carelessness. "There are companies that provide storage for exactly that kind of media and secure that sort of stuff," says attorney **Robyn Meinhardt** with Foley & Lardner in Denver. "People who back up their files can use these companies."

Rule 4: Track Media Containing PHI. Label and classify all PHI-containing media and track such media until their destruction or deletion is secure. Recently in Phoenix, county government sold surplus computers. When someone checked to see if the PHI data had been erased from the computer hard drives, they found a list of all the HIV/AIDS patients being treated in the county, Meinhardt says.

Rule 5: Help Lost Media Find Its Way Home. If diskettes or CD-ROMs containing PHI have been lost, you can easily create an incentive for their eventual return. One hospital designed a labeling system that included a reward for returned media.

Rule 6: Portable Computers Present High Risks of Disclosure. Make sure your computers -- portable or not -- are at least password-protected with "two-factor authentication," so you need a password and a user name, Meinhardt says. "Don't just use your name or something that someone can guess," Meinhardt says. "There are a number of password-cracking software programs out there. So you probably need at least a six-, probably an eight-letter password with a

mixture of numbers, capital letters, and noncapital letters.

"And don't put your password on a sticky on your computer," Meinhardt says.