Risk Tip: Disposing of Old Computers or Copiers

Take these steps to protect patient and practice confidential information before disposing of the equipment.

If you are upgrading to a newer computer or copier, be aware of any confidential information stored on the old system before you dispose of your computer or copier. The following suggestions may help prevent this information from falling into the wrong hands.

Security Issues with Computers

Your computer likely includes confidential patient healthcare details and credit card numbers, practice financial data, and employee salary information. That's why it is helpful to take the following precautions if you are changing your practice computer system:

Back It Up

The first order of business in disposing of your old computer is to back up the files you want to keep. Your owner's manual, the manufacturer's website or its customer support line can provide guidance on saving data before you transfer it to a new computer, CD or flash drive. (Also, check with your state board to determine how long you need to keep practice records.)

What's more, it is a good idea to keep your old computer for a few weeks when converting to a new system. Scott Mooi, a network administrator at Professional Solutions Insurance Company (PSIC) advises: "Sometimes, documents are missed during the back up or the conversion process. If you keep your computer, you can restore necessary documents if you discover you need them later."

Destroy the Hard Drive

Even when you "delete" files, the information could still be recoverable. Hard drives are relatively inexpensive, and it may make sense to simply destroy your old one, if you own the computer.

If you remove the hard drive from your computer before selling, donating or disposing of it, no one will have access to your data. Services are available to shred hard drives. Or, you can destroy it yourself by drilling it full of holes.

Wipe Your Hard Drive

If you lease your computer, you may not be able to keep or destroy your hard drive before you return it. In that case, make sure to "wipe" the hard drive before the computer leaves the premises.

Wiping or scrubbing your hard drive involves deleting all of its files and following up with a program that overwrites all the data with ones and zeros. Contact your vendor or IT consultant for utility programs to permanently delete the files on your old hard drive.

Additionally, commercial security products often provide file wiping capability. Some utilities will erase the entire hard drive, others will erase selected files. They also differ in how thoroughly

they erase the data. Some overwrite the hard drive with random data multiple times, others just once. “Consider using a utility that erases and overwrites the data multiple times,” Mooi suggests.

Privacy Risks Posed by Copiers

Many physicians are surprised to learn the hard drives of many copiers retain images of everything copied. Commercial copiers have come a long way. Today’s generation of networked multifunction devices—known as “digital copiers”—are “smart” machines used to copy, print, scan, fax and email documents.

Digital copiers require hard disk drives to store data about the documents it copies, prints, scans, faxes or emails. If you don’t take steps to protect that data, it can be stolen from the hard drive. This can happen when a copier you own is discarded or a copier you lease is returned and then refurbished and resold.

It’s important to know how to secure data that may be retained on a hard drive when a copier is returned after a lease ends. Mooi recommends including a contractual clause (or language in the purchase order) that requires the vendor to destroy the data or allows you to keep the hard drive.

Destroy the Data

Many copier companies are aware of issues with hard drives on their copiers and already have a number of security solutions in place. You can purchase an encryption solution for the copier’s hard drive or a program that overwrites data onto the hard drive effectively rendering the images unreadable. These solutions can often be installed on both new copiers upon delivery, as well as on existing copiers already in use.

Another option is to ask the vendor to erase the data on the hard drive or destroy it when the copier is returned. “Request that the service provider produce a signed ‘certificate of destruction’ that includes the model number and serial number of the hard drive before taking the copier’s hard drive off the premises,” Mooi advises.

Keep the Hard Drive

You can include language in your contract that requires that the vendor offer you the hard drive for purchase at the end of the lease. In this case, ask for the vendor to send a technician at the end of the lease to come and remove the hard drive.

Issues with Other Office Equipment

According to Mooi, security problems may also exist with printers, fax machines, scanners and even smart phones. Your supplier or cell phone service provider should be able to tell you whether your devices use or store information. “If so, remove any memory device prior to disposal,” Mooi suggests.

Trust is Key

Remember, even if no confidential information is removed from your practice's computer, copier or other equipment, you'll earn patient, client and employee trust by taking the appropriate steps to protect their information.