Develop a Data and Device Destruction Policy in Five Easy Steps

Cheryl Toth*

Destroying and disposing of data or devices that contain protected health information is an essential part of a practice's privacy and security procedures. It also is critical to managing financial risk and risk to your practice's reputation. Many practices, however, have not developed a policy or process for safely discarding the data, or the devices on which the data resides. This article covers five key action steps a practice can take to mitigate the risks involved in destroying and disposing of clinical and financial data.

KEY WORDS: HIPAA; data security; device security; data disposal; policy; medical records risk management.

*Senior practice management and digital media professional, KarenZupko & Associates; e-mail: ctoth@karenzupko.com.

A neurosurgeon who relocated from California to Indiana engaged an off-site records company to store his patient charts. Years later, the physician got a call from a police officer, who told him that loose papers from those medical records had been found along a California highway. Presumably, they blew out of a truck that was transporting the paper, which had clearly not been shredded first. But no one knew for sure.

Yes, this is an extreme case. But it illustrates an important point: You can't predict who might someday end up with your confidential patient information, where it will go, why it will be there, or which patients might be harmed because of it.

To avoid unintended disasters, you need a plan for properly deleting, sanitizing, and disposing of all sensitive patient data and data storage devices. Today.

But although physicians and administrators have the best intentions for protecting patient data, few have a policy and procedure for doing so.

"I think we've lost sight of the big picture," says Michael Sacopulos, attorney and founder of Medical Risk Institute in Terre Haute, Indiana. "People think this is some kind of regulation they must follow. But the privacy and security of clinical data has always been a foundation of good patient care."

Sacopulos believes practices have a responsibility to do everything possible so patients feel that their medical data are safe and secure. "I honestly believe that this is a patient care issue. If a patient thinks his information might get lost, he may not tell a physician something that's critical to getting the right care. That's bad for the patient, and bad for the practice," he says.

The good news is, unlike other policies your practice needs, a data and device destruction policy is refreshingly easy to pull together. It won't take you that much time, and the legal review fees are minimal compared with those for heftier policies, such as an employee policy manual.

WHAT'S THE REAL RISK?

"There is huge reputational and financial risk associated with failing to delete or dispose of data properly," Sacopulos says. "Do you want to be the practice with the mandatory newspaper notice that says: '*We lost our patient data'?* I doubt it."

In an era when patients are shouldering more of the financial responsibility for their healthcare, they have more incentive than ever before to be choosy about where they get care. When your patient data are breached or lost, your reputation takes a hit.

"New data show that 30% of patients will not come back to your practice if they know you've had a breach of their information," Sacopulos says. "And that's if *you* tell them. If they hear about it from someone other than your practice, 60% don't come back. This is compelling because that kind of patient loss creates major financial damage for a practice."

Other financial risks include the cost of penalties and fines—but frankly, just the cost of the breach itself is a financial nightmare. According to Sacopulos, add up mailing costs, protection plans, attorney fees, and other activities, and it's about $160 to $180 per head.

MINIMAL EFFORT, MAJOR RETURN

Enter the data and device destruction policy. "The amount of risk reduction you get from this policy, when compared to the small effort it requires, is astounding," Sacopulos says.

Here's how to develop one in five easy steps. "The general idea is to list all the places where patient data can be found, and make a plan for how they will get rid of it or destroy it when that data is no longer needed," Sacopulos explains. "This can be done by a team within the practice, without any outside help."

1. Make a list of every place that data physically reside in your office.

"I call this the 'Where's Waldo?' exercise," quips Sacopulos. "Laptops, desktops, flash drives, CDs, paper charts—these things are obvious. But not so obvious are things like voice mail, digital cameras, and photocopiers, fax machines, and medical equipment like x-ray machines that have a hard drive. Also, the physicians' mobile phones are often overlooked because they are the physicians' personal property." Use the list below to drive the "Where's Waldo?" discussion in your practice:

- Desktop and laptop computers;
- CDs, DVDs, external hard drives;
- USB disk or flash drive or any devices with storage capacity;
- Printer, fax, and copier hard drives;
- Mobile devices and mobile phones;
- Removable electronic back-up tapes or disks;
- Medical equipment hard drives;
- Digital camera hard drives and data cards;
- Digital photo and imaging systems;
- Voice messages/voice mail; and
- All papers and forms that contain patient medical or financial data.

2. Make a list of the data and devices that business associates have access to or that are maintained or stored by the vendor.

"The average practice has a dozen business associates," Sacopulos explains. "Studies show that business associates are at fault in more than half of all patient data breaches. It's much more likely that a business associate will breach your data than someone in your practice will."

One of Sacopulos' clients thought the collection agency it fired eight years earlier was ancient history—until the administrator was called and told that they agency's server had been stolen. "There was nothing in place that required the agency to delete data from its system, and the company wasn't motivated to clean up old files. It was an eight-year fuse that finally went off," he says.

And some business associates end up being plain old crooks. An orthopedic practice in North Carolina outsourced the digitizing of its x-ray films so they could be transferred into the new electronic health record, then destroyed. "X-ray film contains 4% to 5% silver, and the company had a silver scam going," says Sacopulos. "The company removed and took the silver, and rode off into the sunset with the films." Although there weren't any federal or state fines, it cost the orthopedic practice more than six figures to notify 30,000 patients, purchase identity theft protection, and perform other breach notifications.

Contact each business associate and get the details about how it will dispose of your data and devices if the relationship is terminated. "Ideally, your business associate agreement spells this out for each vendor," says Sacopulos, "but many fall short in this area, so you'll probably have to contact each business associate for these details."

3. Develop the who, what, when, where, and why of how data will be deleted and devices destroyed.

Take your list of all devices and business associates that contain or have access to your data, and for *each device*, answer these questions:

- What is the type of device (e.g., flash drive)?
- What kind of data is stored on it?
- What is the level of sensitivity of that data (high, moderate, low)?
- How do we destroy or dispose of the data?
- How do we destroy or dispose of the device?
- Who does this?
- How often?
- How do we verify that the data and the device are really destroyed?

"I suggest that practices treat all patient data as if it were low-grade radioactive," Sacopulos says. "But the truth is, some data are more sensitive than others. Social Security numbers and financial data, for example, because of identity theft. Certain diagnoses. The efforts you make to destroy the data should be reasonably matched with the sensitivity."

For example, shredding all paper documents, no matter how sensitive the data, makes sense, because it's easy and cheap. But paying for a data deletion certificate for every type of hard drive data wipe is probably overkill. A data deletion certificate is something most IT firms or your IT consultant can provide after they wipe the hard drive. It certifies that the device is completely "clean," and all data are gone. It costs a little extra, but for highly sensitive data, or if you absolutely want to make sure the data are gone, it's a prudent choice.

Beware of "Benign Neglect"

Donating computers and other electronic devices to charity is a common and generous act. Recycling is too. What harm could possibly come from these things?

Actually, a great deal of harm, if those computers or devices contain patient or other confidential data, and they haven't been properly wiped clean.

Every computer or electronic device that gets donated or recycled or given to someone outside the practice should have a data deletion certificate. No exceptions.

"I don't recommend getting a certificate for a camera that took photos of people's rashes on their arm," Sacopulos says. "It's a low risk that someone will do anything with psoriasis pics. But it's different if you're deleting financial data or records containing names of patients with HIV. And never, *ever* donate, recycle, or resell a computer unless you have a certificate. These certificates are a relatively inexpensive way to push liability away from the practice. They also indicate that the practice has gone to great lengths to remove all traces of sensitive data from devices before they are disposed."

4. Draft the policy.

At this point, you're ready to write. The policy should be approximately three to four pages long. Include the answers to these questions in your prose:

- What is the process for shredding and disposing of paper? Do you use a service?
- What is the process for deleting/sanitizing data from each type of electronic media?
- Which data removal software tools are used (e.g., Darik's Boot, Nuke, Blancco)?
- How are CDs, flash drives, removable hard drives, computers, and other media completely destroyed and rendered unusable?
- Who makes sure cell phones and mobile devices are turned in and properly disposed of?
- Who is responsible for deleting, destroying, and discarding data and devices? How is this done (e.g., office shredder, shredding service, disk destruction service)? How often?
- What types of sensitive data or devices require that we obtain a data deletion certificate?
- Which third party is used to obtain data deletion certificates?
- By whom and how is it verified that data have been destroyed? How frequently is this done? In which circumstances do we get these verifications?
- What is the process for verifying that data are wiped or devices are destroyed? Who is responsible for verification?
- Who is responsible for making sure staff and physicians understand this policy and that it is enforced and updated?
- Who must comply with the policy, and what happens if they don't?

5. Hire an attorney to review the policy.

Having an attorney review the policy mitigates the risk of overlooking something important, such as a state-specific statute or using language that is not in your best interest. "This policy is a straightforward review for an attorney," says Sacopulos says. "The cost should be relatively low, somewhere in the range of $150 to $500, depending on your geographic location," Sacopulos says.

CONCLUSION

"Practices already know that if data get into the wrong hands, it's awful for patients and embarrassing for the practice," Sacopulos says. "You don't need a federal regulator telling you that destroying confidential data is the right thing to do."

So take a few hours and get a data and device destruction policy in place. You'll sleep better knowing your patients are protected.