Bouncing Back From a Burglary: How to Survive a HIPAA Nightmare

BY LESLIE BURLING-PHILLIPS, CONTRIBUTING WRITER
INTERVIEWING ANGELA DINH ROSE, MHA, RHIA, CHPS, JEFFREY P. EDELSTEIN, MD, MICHELE G. THOMPSON, JD, AND H. JAY WISNICKI, MD

Threats to the security of patient data can take many forms, such as computer hacking, theft of a laptop from your car, or burglary of your practice, to name just a few. And while practices can make it less likely that patient information falls into the wrong hands, they can't eliminate the risk altogether. What differentiates one practice from another, however, is "recognizing the threat and preparing for it before it occurs," said Jeffrey P. Edelstein, MD, an oculoplastics specialist in Chandler, Ariz.

Last spring, after theft of a computer server, Dr. Edelstein was able to continue patient care with minimal interruption thanks to the precautions he had already taken. Nevertheless, the event triggered a cascade of actions mandated by HIPAA. He shares his experience to highlight how deeply the regulations can affect your practice.

Data Loss Can Happen to Anyone

Despite having a comprehensive security plan in place, Dr. Edelstein had an unpleasant surprise last spring. "When I entered my practice at 8 p.m. on Memorial Day, I may have interrupted a crime in progress. The doors were open. The lights were on. Multiple items were missing—including our computer server," recalled Dr. Edelstein. "We were able to fully restore all stolen data within 48 hours of the robbery. However, it took months to navigate through, and fulfill, all the HIPAA requirements. What's more, the psychological impact was enormous for patients, staff, and myself."

Be Aware of Your Obligations

Most practices are well versed in HIPAA guidelines regarding patient privacy; however, in 2009, the HITECH Act introduced significant changes and additions to the obligations placed on health care entities to protect patient information.

Notify patients about breaches and potential breaches. "A *potential breach* occurs when an unauthorized person can potentially access patient data. For instance, a stolen computer contains HIPAA-protected data, but the database is multilevel-password protected, which may prevent data from being accessed," said Dr. Edelstein. "In contrast, an example of a *breach* would be if a computer expert or hacker broke into or bypassed password-protected systems using the data for activities such as identity theft."

Under the HITECH legislation, "providers are required to notify patients about breaches or potential breaches of that data," said Michele G. Thompson, JD, a partner at the Udall Law Firm in Tucson, Ariz., who specializes in health care law and regulatory violations. An exception to this duty of notification occurs if the data are encrypted, said Dr. Edelstein. "However, most software vendors do

Notifying the Media

If more than 500 patients are affected by a breach or a potential breach of patient data, you are required to contact the media. "Within hours of issuing my press release, I was contacted by KPHO TV for the interview to be aired on the evening news," said Dr. Edelstein. "I had less than 10 minutes to prepare for an interview. I felt fortunate that I attended several Academy media training seminars because I had learned to focus my response on the important points of the story. I relayed my concern for patient privacy, identity theft, and the personal safety of my staff. Furthermore, I explained the positive steps taken to prevent a similar theft in the future. Finally, I described the details of my subspecialty practice and how the local community benefits from my participation with the Barrow Craniofacial team and the NHL Phoenix Coyotes hockey club."

AMERICAN ACADEMY OF OPHTHALMIC EXECUTIVES
Solutions for Practice Management

Each month, Practice Perfect addresses one of the AAOE's seven key competencies.

not currently use encryption due to issues of speed and data access."

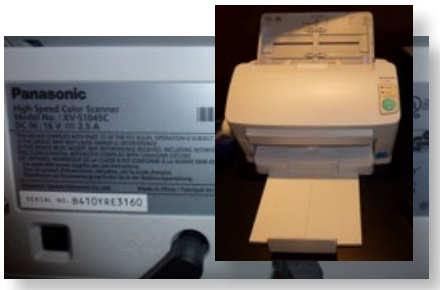
Understand that you may be subject to an investigation. The 2009 legislation "also allowed state attorney generals to prosecute those who violate the regulations," said Ms. Thompson. "Failure to follow these statutes can lead to an invasive investigation of your practice, a civil lawsuit may be filed for negligence, and costly fees and penalties could be assessed if a patient's information is compromised." Prosecutions are most likely to take place in cases where the loss of data has been negligent or willful, said Dr. Edelstein. "For instance, leaving your laptop on an airplane, or an unhappy ex-partner stealing patient lists without proper authorization"

Know the HIPAA regulations. "Unfortunately, not all administrators realize the level of compliance that a practice must attain," said Angela Dinh Rose, MHA, RHIA, CHPS, director of Health Information Management Solutions at the American Health Information Management Association. "Small practices, in particular, barely get beyond the basics. For example, the law requires that every entity appoint a privacy and security officer—someone responsible for creating policies, training, and handling complaints, for example—but many practices do not." Practices should also be aware that it is the physicians generating the patient data who are at risk, no matter where it is stored, added Dr. Edelstein. "For example, physicians using a third-party vendor to store data on a 'cloud-based' network may share some risk for the HIPAA violations associated with a breach of that network."

What You Should Do Now

"Providers must have certain security procedures in place and a written policy that details those precautions," said Ms. Thompson. "The three core areas to address are 1) administrative, 2) technical, and 3) physical."

1. Address administrative issues. HIPAA requires entities to perform a risk analysis to determine possible vulnerabilities.



BE READY TO REPLACE EQUIPMENT. Take a thorough inventory of all the equipment that you might need to replace. Digital images that include the model number and serial number of each device, along with receipts, can help you provide police and insurers with the information they need.

Use your HIPAA risk analysis. Develop organizational policies based on what you learned from the risk analysis. You also should hold regular training sessions for employees to emphasize the importance of, and methods for, keeping patient data secure.

Itemize everything that you might need to replace. "Save and organize the receipts for each piece of equipment purchased for your office. This includes autoclaves, computers, cameras, and anything else you may have to replace after a burglary," said Dr. Edelstein. "A digital photograph is an easy way to store and quickly retrieve critical data necessary for police reports and insurance verification of stolen items. Photograph the front of the item, as well as the tag with the serial number and model number on the back. This may lead to the return of your property or the identification of the thief, should he or she take it to a pawnshop." In some jurisdictions, pawnshops are required to compare the serial numbers of goods against an international police database.

Make sure you are insured. Replacing stolen items is expensive. Responding to occurrences of compromised patient information can be even more costly, particularly if you are targeted for an investigation. "Purchase insurance to replace your property and add a rider to your policy to cover expenses you will incur while meeting HIPAA obligations, should a security breach occur," said Ms. Thompson. "Replacement-cost insurance is helpful, and riders may cover the technical costs of urgent server replacement, data recovery, and restoration," added Dr. Edelstein.

2. Apply electronic safeguards. Practices should have a number of electronic measures in place to keep patient data secure. "If your computer is stolen, the hard drive can be reformatted and used as if it were new, but a thief will be unable to access sensitive data if you follow certain guidelines," said pediatric ophthalmologist and information technology (IT) specialist H. Jay Wisnicki, MD. He described 10 actions a practice should take to keep patient data electronically secure.

Avoid laptops and plug-in data drives. "Desktops can be stolen, but portable devices are at a higher risk. If you must use them, make sure they are kept secure," he said.

Require a password login to networks, individual computers, and software. "Passwords should include a combination of letters, numbers, and punctuation."

Keep passwords secure. "Passwords should be kept private. The last thing you want employees to do is post their passwords on their computer screens."

All computers should have automatic time-outs. "Computers storing patient data should be configured to 'time out' when inactive, with a password required to log back in."

Deactivate passwords when employees leave the practice. Make sure this is part of your office procedures.

Install firewalls. Be sure to keep the firewall software updated.

Limit employees' Web browsing. "Not all websites are secure. Viruses and malware can compromise your data or render it unusable or inaccessible," he said.

Install antivirus software. Make sure you keep it up to date.

Be careful with patients' financial information. Do not keep patient credit card numbers on file.

Back up your data frequently. "The more often you back up your files, the better. This ensures that the most current data can be restored if necessary.

And store a copy in a secure location away from your practice, but close enough so that it is easily accessible if needed," he said.

3. Secure the premises. "Our response to the theft was to dual-lock the computer room and install a more robust alarm system," said Dr. Edelstein.

Limit access to your server. Consider that "anybody with access to your office is a potential threat. Access to your computer room should be restricted to IT, practice administrators, or owners. It is an unnecessary risk for building management, cleaning crews, or noncritical employees to have access to your server," said Dr. Edelstein. "Nobody has access to my computer room except myself."

Use video cameras. Video surveillance serves as a deterrent. Inexpensive video systems allow you to identify intruders from your cell phone, and most important, said Dr. Edelstein, it allows you to see inside the premises before you enter at nonstandard times, such as weekends or evenings.

What to Do After Data Loss

Even those with the most sophisticated security plans can suffer a security breach. How you respond to that breach can significantly affect your business. "Even though I was a victim and was not at fault for the security breach, I was concerned about my patients' response and how my practice and reputation might be affected," said Dr. Edelstein.

Consult an attorney. After the police are notified, contact an attorney who specializes in health care regulations and violations to guide you through the regulatory requirements of patient notification. "Contact an attorney immediately because entities are obligated to notify patients of a breach or potential breach of data within 60 days. Although this may seem like plenty of time, the process can be lengthy. For instance, an internal investigation may be necessary to determine how the theft occurred and to confirm how many patients were involved," said Ms. Thompson. "The Ophthalmic Mutual Insurance Company has HIPAA insurance to help in this situation," said Dr. Edelstein. "OMIC set me up with attorneys who specialized in HIPAA issues."

Notify your patients and your community. Once you gather all the pertinent information, write a letter to your patients and draft a press release (see "Notifying the Media"). "Craft these in such a way that you answer all the questions that patients might have," said Dr. Edelstein. "For example, 'What is the likelihood that my information has gotten into the wrong hands? Why did this happen? What will be done to prevent this from happening again?' I gave them all the information they needed to understand and properly respond to the situation, and I conveyed that I was advocating on their behalf." Both the letter the press release should include:

- What happened
- What type(s) of protected health information were involved (e.g., date of birth, diagnoses)
- Steps patients should take to protect themselves (e.g., place a fraud alert on their bank account)
- How the provider is investigating the breach (e.g., police investigation)
- What has been done to mitigate the harm
- What the provider is doing to protect against future breaches
- Contact information for the provider so individuals can call or write for more information

Hire a call center. Consider hiring a call center to handle patient questions, "especially if your practice is small, so your staff is not inundated with calls. To help staff at the call center answer questions, create a list of 'talking points' similar to those used in your notification letter and press release. Expect 10 to 20 percent of patients to get in touch for more information," said Ms. Thompson.

"Make sure the call center immediately forwards the names of any unhappy patients with details of their concerns and their specific needs for resolution," said Dr. Edelstein. "We had only one unhappy patient out of 5,000 notifications."

It Could Have Been a Lot Worse

The burglary and its aftermath created a great deal of stress, but Dr. Edelstein's precautionary measures meant that he was able to quickly reconstruct the database (without any loss of data) on a temporary server. He later transferred the data to a new replacement server. His precautions also made it easier to replace the stolen equipment. And although the loss of the computer server constituted a potential breach of patient data, there was no evidence of an actual breach after six months of follow-up.

Back Up Your Data

Theft, fire, hardware failure, database corruption—there are many unwelcome surprises that can result in loss of patient data. If you want to make sure your practice is ready to bounce back, "the number one issue is to have daily backups stored in multiple locations. And rather than overwriting the previous day's backup, keep multiple backups," said Dr. Edelstein. "You are only as safe as the latest working backup you have. The fewer backups, the greater the potential for real data loss."

What data should you back up? When backing up data, save everything that is important to the operation of your practice. "In addition to patient information, include all of your forms, manuals, contact lists for vendors, custom templates, promotional materials, business cards, educational materials, and QuickBooks, for example," said Dr. Edelstein. "It takes considerable time to compose and collect this information and would be extremely inefficient to re-create it."

How is your vendor backing up your data? "Talk to your vendors to make sure you are backing up your data correctly," said Dr. Edelstein. "Ask your vendor: 'If this computer is lost, stolen, or corrupted, what is needed to get up and running per our latest backup?' And test the system occasionally to confirm it works as expected."