Medical EconomicsData security

7 tips to protect patient data from visual hacking

November 07, 2016
By Milly Dawson

With a major hack of an insurance company's database having made front-page news not long ago, it's natural that many physicians think first about electronic data when they think about protecting patients' private health information (PHI).

Related: Ethical hacking a vital necessity to fight against healthcare randsomware

However, low-tech violations of patient data actually occur far more often, have the potential to cause harm and, sometimes —though very rarely—incur serious penalties. So-called visual hacks can occur when employees leave paper records on a desk or allow a monitor to be casually seen. Such low-tech slips occur often, and they warrant both concern and preventive action.

Luci Belnick, MD, who independently practices internal medicine in Orlando, Florida, acknowledges how easily slips can occur.

"When you bring the next patient into your exam room, once in a while, you might have left the last guy's note open" on the monitor, she says. "I try not to, but once in a while it happens."

In 2011, an employee of a physician group associated with Massachusetts General Hospital left a file holding paper records of 193 patients, many with HIV/AIDS, on the subway. The hospital paid a $1 million fine.

Further reading: Tips to improve cyber security and protect your practice's finances

Belnick says she spends about 20 hours weekly updating medical records. She notes that for doctors who have long commutes on busses or trains, using that time for record-keeping may be unavoidable.

She has worked on patient records on airplanes, she says, folding a magazine over the top of her laptop to block the patient's name from her seatmate's view.

Next: Avoiding common security lapses

Small lapses, the commonest kind

Dennis Melamed, who publishes a newsletter called Health Information Privacy/Security Alert, says that while visual hacking, including lapses that involve paper records, don't get much attention, such breaches are actually the most common.

Exclusive: 2016 EHR Report

Kate Borten, of The Marblehead Group, a healthcare security and privacy firm, agrees.

“Though the press focuses on a big insurer losing control of millions of records, recent academic research confirms that the vast majority of healthcare breaches involve smaller numbers of records,” she says.

Simple steps to keep confidential data confidential

Here’s how to prevent most visual hacking:

1. Adopt an office-wide clean-desk policy. Have everyone handling PHI remove papers from their desks and close records on monitors each time they step away. Also, have papers kept in folders when not in use, and files stashed in cabinets or drawers. Be sure to promptly pick up papers from fax/copier/printer devices.

2. When possible, see that doors to offices are shut.

3. Limit access to areas with computer monitors or workstations that display PHI. Position monitors so that the data is easily viewed only by the person directly in front of that monitor. If necessary, use privacy filters to keep unauthorized persons from viewing monitors inappropriately. These block peripheral reading of the screen by anyone not positioned directly in front of the monitor. Borten says that soon-to-be-released technology will have a built-in electronic screen that a user enables or disables with a keystroke.

Next: More security tips

4. Ensure systems that display PHI on monitors have an automatic shutoff feature that kicks in when there is no activity.

5. Be aware of others close to you when you are working with PHI on a mobile device outside of your regular work environment. Protect device screens from unauthorized views everywhere, not just in the office.

6. Train staff not to be too trusting. Someone may show up claiming to be from IT, and wanting to be nice, your office staff may not question them. Educate staff to make certain that anyone requesting access is entitled to it.

7. To ensure proper procedures are being followed, schedule regular walk-throughs.

Melamed says that it’s hard to prove harm when privacy violations occur, and that the real risk to a physician’s office is that if a patient lodges a complaint, the Office for Civil Rights under HHS will investigate—asking about your policies and training to control access.

Technology: 5 tips for tactfully combatting negative patient reviews

If you can show your office has taken practical steps, you should be fine, even if an occasional slip has occurred, says attorney Neal Eggeson, JD, an Indianapolis-based expert in privacy law and medical malpractice.

“HIPAA does not require perfect privacy protections —only reasonable safeguards,” he says.