How to protect valuable patient data

Encryption, passwords essential lines of defense, experts say

By **MICHAEL McBRIDE,** *Technology Editor*

POWER POINTS

- **Electronic health record systems pose a security risk that can damage your practice if you don't take adequate precautions.**
- **To comply with Health Insurance Portability and Accountability Act requirements for privacy and security, first conduct a security risk analysis.**

A medical student trainee at the University of Texas MD Anderson Cancer Center boarded an employee shuttle bus on July 13, and when she exited, she left behind a portable hard drive that contained the unencrypted protected health information (PHI) of 2,200 patients. It was never found.

Earlier this year, an MD Anderson faculty member's laptop was stolen during a home burglary. It contained the unencrypted PHI of more than 30,000 patients, including their names, treatment data, and (for some of them) their Social Security numbers. The laptop was never recovered.

These kind of incidents are not uncommon. In the past few years, healthcare providers all over the country have experienced PHI security breaches because computer hardware was either lost or stolen. The questions are, why was the PHI was there in the first place, and why was it not encrypted?

The Health Insurance Portability and Accountability Act (HIPAA) holds physicians accountable for the security of their patients' PHI. Federally authorized certification organizations such as the Certification Commission for Health Information Technology ensure that electronic health record (EHR) systems comply with current rules and regulations covering the use of PHI.

Simply having a HIPAA-compliant EHR, however, does not guarantee the security of your patients' medical records. For that, you must take specific steps and accept personal responsibility.

DOCTOR VULNERABILITY

Primary care practices are especially vulnerable to security breaches, says Sean P. Kelly, MD, a board-certified emergency medicine physician who practices and teaches at Beth Israel Deaconess Medical Center in Boston, Massachusetts. That's mainly due to the large amount of data exchanged internally between practice departments, as well as externally with hospitals, specialists, health plans, home health organizations, hospices, physical and occupational therapy offices, and other external care providers and payers.

"Whenever data are exchanged, practices are vulnerable," Kelly says. "Especially with elements that are part of protected records such as HIV status, psychiatric, and other chronic diagnoses that might not be specifically relevant to the patient's immediate healthcare needs."

This issue is of particular concern in the claims submissions process, where administrative assistants might submit information to billing agencies or insurance companies to justify payments for services or equipment or to receive pre-authorization for tests that might also include other privacy protected PHI.

UNDERSTANDING HIPAA

Rebecca Herold, CISM, CISSP, CISA, CIPP, FLMI, is an information security, privacy, and compliance consultant, author, and instructor who has provided assistance, advice, services, tools, and products to organizations in a wide range of industries, including healthcare, for more than 2 decades.

She blames lack of awareness of HIPAA requirements and the inherent opportunities to mishandle PHI for most of the recent breaches in PHI security at hospitals and in primary care practices. Herold notes the following categories where physician education and implementation of security

protocols can prevent exploitation of lax PHI security.

Device encryption

Studies such as "How mobile devices are transforming healthcare," a recently released report from the Brookings Institution's Center for Technology Innovation, indicate that more and more physicians are using mobile devices in their practices and at the point of care.

Researchers estimated that as much as two-thirds of the mobile medical device market soon will be comprised of remote healthcare-related technology for managing chronic diseases.

This change can be a boon for doctors who want to carry patient records with them as well as receive alerts and test results immediately. Many physicians, however, are not aware that to fully comply with HIPAA as well as the PHI policies of the hospitals where they work or have privileges, the PHI stored on their mobile devices must be encrypted.

"Many [physicians] believe that they have good personal habits that will not lead to the devices being lost or stolen," Herold says. "However, the long and growing list of incidents involving such lost and stolen devices demonstrates otherwise."

Herold says "many to most" doctors regard encryption as too cumbersome and complicated to use, or they believe that it's not necessary for mobile computers and storage devices. Both assumptions could lead to lost or stolen PHI. Serious breaches have resulted in steep fines levied against physicians, and even lost privileges.

Transmitting PHI

HIPAA also requires PHI to be encrypted when it is transmitted through public networks from one system or device to another.

"Many [physicians] believe that encryption is not necessary for PHI being sent in e-mails," Herold says. "I've heard some [doctors] express disbelief that it can be intercepted at all, simply because they haven't seen hard data on the problem. E-mail interceptions, however, don't leave digital trails, so the amount of information taken this way cannot be determined. It is, however, a very real risk that's been confirmed by many security organizations."

Restricted PHI

Medical records are not just accessed by physicians. Nurses, administrators, techs, physician assistants, check-in/registration personnel—nearly all staff members—access PHI throughout a working day.

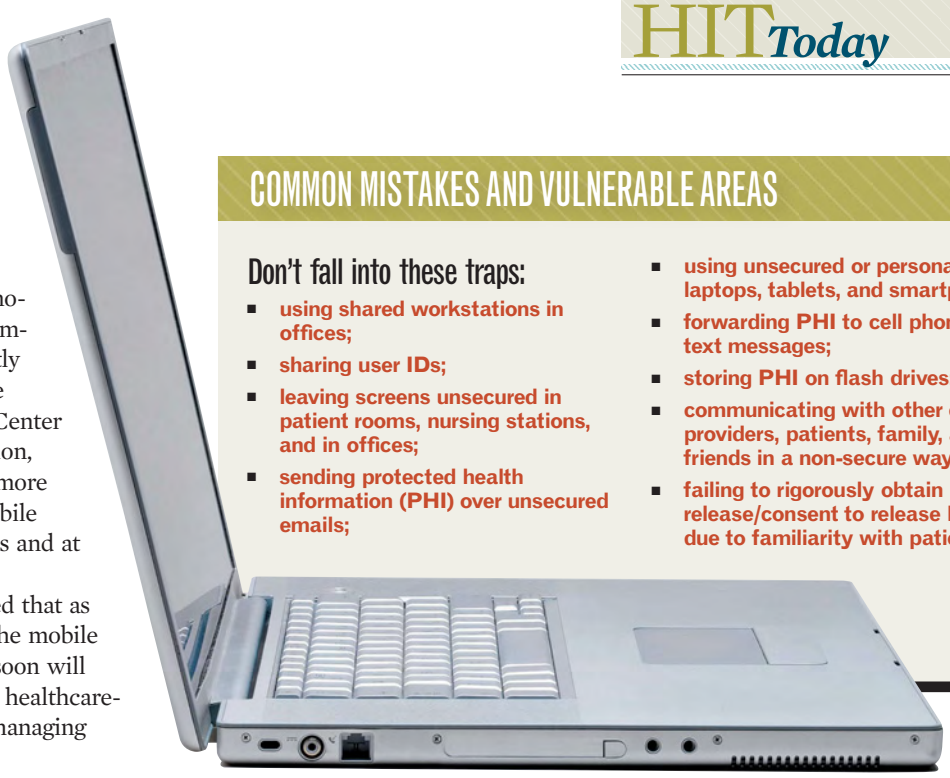
To be HIPAA-compliant, a practice must have a minimum set of technical controls that establish parameters to the ingress and egress of patient records.

"There's a tremendous amount of information being sent around the system by nurses and administrators in the name of the primary care physician [PCP] without the PCP being able to thoroughly review it," Kelly says. "The EHR is a tremendous treatment and communication tool, but who should receive what information? A busy [PCP] or specialist cannot spend time redacting sensitive patient information."

Kelly notes that much of the PHI embedded in patient records should not be accessible to third parties when physicians submit their reimbursement claims. But how can a doctor control that? For example, is a physician responsible for protecting a patient's privacy related to a previous treatment for depression or HIV when submitting a workers' compensation claim?

"The reality is that patient-sensitive information is embedded into a good clinical record. It is not an isolated data set," Kelly says.

According to Herold, many of the



COMMON MISTAKES AND VULNERABLE AREAS

Don't fall into these traps:

- using shared workstations in offices;
- sharing user IDs;
- leaving screens unsecured in patient rooms, nursing stations, and in offices;
- sending protected health information (PHI) over unsecured emails;
- using unsecured or personal laptops, tablets, and smartphones;
- forwarding PHI to cell phones as text messages;
- storing PHI on flash drives;
- communicating with other care providers, patients, family, and friends in a non-secure way; and
- failing to rigorously obtain proper release/consent to release PHI due to familiarity with patients.

"There's a tremendous amount of information being sent around the system by nurses and administrators in the name of the PCP without the PCP being able to thoroughly review it."

—Sean Kelly, MD

GETTY IMAGES/STOCKBYTE/GEORGE DOYLE

"A comprehensive security and privacy program is legally required. [Physicians] do not have a choice about compliance."

—Rebecca Herold, CISM, CISSP, CISA, CIPP, FLMI

doctors who practice medicine with her healthcare-provider clients get frustrated with the controls preventing them from accessing complete medical records.

"They want access to all records on their patients," Herold says. "They say that their medical ethics pledges will prevent them from viewing unrelated data; however, depending on system users to simply not look at private records is not an acceptable or effective means of control. It certainly would not pass an audit."

Password management

Physicians, according to Herold, seem to abhor having to input passwords to log onto computers and into hospital networks. Their reasons range from "They slow me down" to "They don't contribute to good patient care." And yet passwords are the first line of defense against security intrusions.

"All the physicians I've spoken with have a huge dislike of passwords," Herold says. "They don't like having to use them, they don't like having to occasionally change them, and they usually don't safeguard them appropriately. One physician told me that being forced to change his password every 90 days was unreasonable. He even admitted to keeping a list of passwords on his computer where his patients could see it."

She adds: "Physicians often believe they already possess all the knowledge necessary to safeguard patient information. And they often tend to be completely trusting of everyone within their facilities, so they don't implement the appropriate physical controls. They need to realize the vast amount of risks that exist and be more cooperative with their information security and privacy folks. They also need to understand that a comprehensive security and privacy program is legally required. They do not have a choice about compliance."

HOW TO ENCRYPT DATA ON COMPUTERS, MOBILE DEVICES

Encrypt your data now and take one vital step toward Health Insurance Portability and Accountability Act compliance. These companies offer free open-source encryption software for Windows, Mac OS X, and Linux operating systems, and online you can find additional companies offering such services. Use them to encrypt data on hard drives, portable thumb drives, and CDs:

www.truecrypt.org
www.safehousesoftware.com
www.cypherix.com

You can do Smartphone, iPhone, and iPad encryption on your own as well. The following companies offer solutions for encrypting data on your mobile communications device:

www.aikosolutions.com
www.juniper.net
www.apple.com/iphone/business/integration/
www.zenprise.com

SECURING YOUR PRACTICE

Comprehensive data security requires patience and diligence, especially in healthcare, where the technology may evolve more quickly than safeguards can be built to secure it.

Seek out PHI security and privacy experts for guidance. Most hospitals have their own internal specialists who establish and monitor their organization's PHI policies. Solo practitioners and group practices, however, will need to engage the expertise of an outside consultant to establish the physical, technical, and administrative requirements for true PHI security.

"The first step physicians must take is to have a qualified information security compliance professional perform a risk assessment—preferably one who is also a HIPAA expert," Herold says. "From there, they can identify their security weaknesses and work to address them."

Both Herold and Kelly recommend that PCPs become certified for meaningful use applications and systems as soon as possible. They'll then have in place the security controls needed to integrate with the health information management systems used by accountable care organizations and Patient-Centered Medical Homes.

"To comply with HIPAA requirements for privacy and security, physicians must first conduct a security risk analysis," Kelly says. "This involves assessing potential risks to PHI and should include access management (getting in and out of your EHR), workstation security (what happens when you or a colleague walks away from the computer), and authentication at the point of entry, among others."

The sooner you secure the PHI on your practice's computers and mobile devices, the sooner you'll experience the benefits of knowing you've done all you can to prevent the loss or theft of your patient's private health data.

Single sign-on solutions can help. They eliminate the need to remember long-string passwords to gain access to your clinical and business systems. In these systems, caregivers use proximity cards or biometric finger/palm readers to access healthcare networks and move through applications.

Such improvements result not only in HIPAA-compliant security measures but also save you time and hassles—something care teams and information technology personnel alike can appreciate.

Send your feedback to medec@advanstar.com. Also engage at www.twitter.com/MedEconomics and www.facebook.com/MedicalEconomics.