IT Security—What All Orthopedic Surgeons Must Know

Cheyenne Brinson, MBA, CPA

Orthopedic surgeons rely on technology on a daily basis, from using a practice management system for billing and scheduling to (for some) electronic health records (EHR). Walk in to any education session for orthopedic surgeons and more than half the people in the room have a laptop, iPad® (Apple Inc., Cupertino, California), iPhone®, (Apple Inc.) BlackBerry® (Research in Motion, Waterloo, Ontario, Canada), Droid® (Motorola, Schaumburg, Illinois), or other personal digital assistant (PDA). Savvy users access their billing reports or view their office schedule on their PDA. Others chart a patient note from the comfort of their own home, electronically prescribe medications while watching their child's soccer game, or access a patient's chart while on call before leaving for the emergency department. Technology advances continue to streamline once-impossible tasks, heralding a new era of how orthopedic surgeons practice.

ALONG CAME HIPAA

In 2000, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule")[1] established a set of national standards that orthopedic surgeons must follow to protect their patients' personal health information (PHI)—whether electronic, paper, or oral. The Privacy Rule protects all "individually identifiable health information"—that is, any information that identifies the patient's past, present, or future medical condition; the provision of health care to the patient; or the past, present, or future payment for the provision of health care to the patient. This includes a patient's name, address, date of birth, or social security number. The Privacy Rule was issued to implement the requirement of HIPPA (the Health Insurance Portability and Accountability Act of 1996).[2] In practice, the Privacy Rule is synonymous with HIPAA.

Ms. Brinson is Consultant and Speaker, KarenZupko & Associates, Inc. (KZA), a practice management consulting and training firm based in Chicago, Illinois. KZA has worked with thousands of orthopedic surgeons nationwide.

Address correspondence to: Cheyenne Brinson, MBA, CPA, KarenZupko & Associates, Inc, 625 N Michigan Ave, Suite 2225, Chicago, IL 60611 (tel, 312-642-5616 ext 220; fax, 312-642-5571; e-mail, cbrinson@karenzupko.com; Web site, www.karenzupko.com).

Am J Orthop. 2012;41(1):44-46.

Under the American Recovery and Reinvestment Act of 2009 (or commonly referred to as the Stimulus Bill), the Health Information Technology for Economic and Clinical Health Act (HITECH Act) requires practices to notify patients if a breach of "unsecured" PHI occurs. Practices are subject to stiff penalties, ranging from $100 to $10,000 for each violation, up to a maximum $1,500,000. The Act also authorized state attorney generals to bring civil actions for breaches of unsecured PHI.[3] Breaches of unsecured PHI affecting more than 500 people are published on the Department of Health and Human Service's (HHS) Web site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html).

Protecting PHI requires comprehensive policies and procedures. HIPAA policies created 15 years ago are no longer relevant today, as technology usage has increased and patient information storage and transmittal has evolved. Do your privacy policies adequately address your current environment? John Brewer, a physician-practice information technology (IT) consultant and HIPAA educator and trainer, president of MedTech USA, advises orthopedic practices to revamp their HIPAA policies and procedures completely once the practice converts to an EHR and to appoint a HIPAA security manager.

TECHNOLOGY DOES NOT COME WITHOUT RISK

At an alarmingly frequent basis, headlines across America are splattered with the latest public relations disaster regarding another health care privacy breach. From health insurance companies to hospitals to private practices, health care providers are vulnerable to human error that can earn them a spot on the cover of national, state, or local news. Most recently, TRICARE reported the largest data security breach, with misplaced back-up tapes to blame. Nearly 5 million patients were affected.[4] A private practice made headlines when a computer bag with a flash drive containing PHI for 2,200 patients was stolen from a locked car of an employee.[5] These types of headlines remind physicians of their responsibility under the Privacy Rule. Chuck Blazek, Chief Technology Officer at Midwest Orthopaedics at Rush in Chicago, Illinois, understands the importance of IT security and comprehensive IT security policies. As Mr. Blazek sees it, "one mistake and you're on the front page of the Chicago Tribune." And in today's instantaneous information sharing age, that story in the Tribune has just now exploded in the social media circles.

Protect yourself

The good news is, with proper planning and tools, PHI rather easily can be secure. PHI is secure if it is rendered unusable, unreadable, or indecipherable to unauthorized individuals through encrypting, destroying, or purging it from an electronic device.[3] Encryption is defined as an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key (and the process or key has not been breached).

Are your devices encrypted?

Encryption is the key (no pun intended) to securing PHI. The National Institute of Standards and Technology (NIST) issued a *Guide to Storage Encryption Technologies for End User Devices* that describes implementation strategies for encryption solutions.[6] As long as data are encrypted, a lost laptop or misplaced flash drive is not a reportable event under the HITECH Act. "Physicians are a thousand times more vulnerable to a lost or stolen device than having their server hacked," warns Mr. Brewer.

E-mail. As a general rule, PHI should never be e-mailed unless it is encrypted. There are many inexpensive solutions to encrypt e-mail. Midwest Orthopaedics at Rush uses ZixCorp e-mail encryption services for confidential e-mails, including e-mails to case managers. To encrypt and secure e-mail, e-mails are marked "confidential" or the word "confidential" is placed in the subject line. These e-mails cannot be forwarded or saved by the recipient. Additionally, most EHRs offer a patient portal to exchange PHI securely with patients.

Cell phones and PDAs. Password protection is the critical first step in protecting mobile devices. Many mobile devices, including the iPhone and Blackberry, have features that will remotely delete all data stored on a device after too many unsuccessful password attempts. Devices also can be remotely tracked and located on a map. Take advantage of the security measures that are built in to the device.

Avoid storing PHI on a PDA. Nevertheless, it is critical that a PDA be password protected. Mr. Brewer warns, "PDAs are an open hole waiting to be violated." Even when PHI is not stored on the PDA, leaving open the application that runs the EHR is not secure if the device is lost or stolen. Password protection helps mitigate this risk.

Laptop computers, tablets, and personal computers. The best mechanism to secure portable computers is to not save data to them. Rather, store data on a remote system and have users access data through a secured means (VPN, Cloud). The user views and modifies remote data through a Web interface.[6] This is also referred to as "dumb terminals;" if these devices are lost or stolen they do not contain PHI. Midwest Orthopaedics at Rush follows a similar strategy. Their EHR is hosted in a private cloud and none of the workstations have PHI stored on them. This not only protects PHI but also serves their disaster recovery and business continuity plan.

It is especially important in the EHR environment to disable the exporting of PHI to external devices (eg, Universal Serial Bus [USB] flash drives, compact disks [CDs]), unless the data are encrypted on the portable storage device. At a minimum, PHI must be encrypted on any computer. Mr. Brewer finds it safer to encrypt the entire device, not just the folder where PHI is stored.

IT Security Checklist

Work with your IT department or IT provider to ensure:

- ☐ Updated HIPAA policies and procedures
- ☐ Updated IT Security policies and procedures
- ☐ Annual HIPAA training for all staff (physicians, clinical staff, and nonclinical staff)
- ☐ E-mail is encrypted
- ☐ PDAs are password protected and no PHI is stored (unless encrypted)
- ☐ Laptops, tablets, and computers are encrypted
- ☐ USB flash drives, CDs and external drives are encrypted

Figure. IT security checklist. CDs = compact disks; HIPAA = The Health Insurance Portability and Accountability Act of 1996; IT = information technology; PDA = personal data assistant; PHI = personal health information; USB = Universal Serial Bus.

USB flash drives or "jump drives," CDs, and external hard drives. The NIST recommends the use of a flash drive with self-contained storage encryption capabilities, such as encryption software and secure key storage. These can be purchased at any office supply store.

EHR Meaningful Use

Incentive funds are available for physicians who adopt and use an EHR. Among the criteria for establishing "meaningful use," physicians must implement systems to protect privacy and security of patient data in the EHR.[7] As part of the risk management process, physicians must conduct or review a privacy risk analysis of the technology, implement security updates as necessary, and correct identified security deficiencies. They also must update their HIPAA policies and provide HIPAA training to physicians and other staff who handle protected health information.

Conclusion

Mr. Blazek believes too often IT security is an afterthought, when instead it needs to be on the forefront of any IT project from the planning to the implementa-

tion phases. He advises practices to evaluate potential implications of an IT breach. There can be severe consequences, including public relations issues, patient and public trust, and monetary penalties (assessed under the HITECH Act).

Author's Disclosure Statement

The author reports no actual or potential conflict of interest in relation to this article.

References

1. U.S. Department of Health and Human Services, Office for Civil Rights. *HIPAA Administrative Simplification, Regulation Text, 45 CFR Parts 160, 162, and 164.* Washington, DC: U.S. Dept of Health and Human Services; March 2006. http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf. Accessed December 13, 2011.
2. Modifications to the HIPAA privacy, security, and enforcement rules under the Health Information Technology for Economic and Clinical Health Act. *Fed Regist.* 2010;75(134):40868-40924.
3. Office of the Secretary, Department of Health and Human Services. Guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the breach notification requirements under section 13402 of Title XIII. *Fed Regist.* 2009;74(79):19006-19010.
4. Risk to patients from data breach met with proactive response. TRICARE Web site. November 4, 2011. http://www.tricare.mil/mediacenter/news.aspx?fid=738. Accessed December 13, 2011.
5. Petrishen B. Thousands of medical records stolen in car break. *MetroWest Daily News*. October 11, 2011. http://www.metrowestdailynews.com/editorspick_mobile/x1092315665/Thousands-of-medical-records-stolen-in-car-break. Accessed December 13, 2011.
6. Scarfone K, Murugiah S, Sexto M. *Guide to Storage Encryption Technologies for End User Devices. Recommendations of the National Institute of Standards and Technology.* Special Publication 800-111. Gaithersburg, MD: National Institute of Standards and Technology, U.S. Dept of Commerce; 2007.
7. Centers for Medicare & Medicaid Services, Department of Health and Human Services. Medicare and Medicaid Programs; Electronic Health Record Incentive Program. *Fed Regist*. 2010;75(144):44313-44588.