PHYSICIAN'S DIGITAL LIFE

The use of electronic communication is now fully woven into the fabric of everyday life and work. Electronic information and communication requires new ways of thinking about privacy and security. Nevertheless, familiarity with these tools may lead to complacency. Everyone has a story about a "reply all" embarrassment. Taking a moment to consider how digital tools are used may save time and avoid headaches.

First principles

Personally identifiable information about patients can only be disclosed in accordance with their written authorization or for appropriate treatment, payment, and health care operations purposes as disclosed to them in the notice of privacy. The practice must employ appropriate safeguards and security measures to avoid inadvertent or unauthorized disclosures. Technology vendors that store protected health information for the practice must provide a HIPAA business associate agreement.

Email

It is never appropriate for employees of the practice to use their unsecured personal email accounts, such as Gmail or Hotmail, to communicate with or about patients.

Practices that have EHR systems meeting Meaningful Use criteria will have a secure mechanism that patients can use to communicate with the practice. The federal government has issued guidance suggesting that providers who have this facility should favor it over other methods, unless they are certain that those other methods meet security requirements.

Use of other email systems is not forbidden, but does raise a number of considerations. The system must meet HIPAA security rule requirements. Two categories of risk to consider are transmission risk and storage risk.

When an email is sent, there is some risk that it may be misdirected or intercepted. After an email is created or received, there is risk that the computer, server, or media on which it is stored may be lost, stolen, or “hacked”. An email can simultaneously exist in multiple locations, such as server, PC and phone. If more than one person received the email, the number of copies can quickly multiply.

Encryption, while not specifically required by regulation, is a common approach to these risks. Encryption scrambles data so that it cannot be deciphered without a digital “key”, similar to a password. Encryption can be applied to a file, a directory, or an entire device. Depending on the approach that is used, some may find encryption a bit cumbersome. The benefit is that if properly encrypted data is lost, stolen, or misdirected, there is no breach because the encrypted data is unusable without the key.

If email is used to communicate with patients, they should be informed that it should not be used to get medical help in an urgent or emergency situation. There should be clear instructions as to who and where to call for immediate help.

Texting

Texting presents some of the same issues as email, and careful consideration should be given to the risks and benefits. We are aware that some practices use text messaging to send appointment reminders and confirmations. We suggest that patients be given an option as to whether or not they wish to receive text reminders, and suggest that no clinical information, such as reason for visit, ever be put in a text message.

The federal government issued guidance reminding that the texting method must comply with the HIPAA security rule.

The text conversation may escalate from a routine appointment reminder to something more sensitive, such as the patient responding with a report of a new symptom. Bear in mind that while the patient is not bound by HIPAA privacy and security rules, the practice is. Just because a patient elects to provide sensitive information via an unsecured text message does not mean that the practice is free to respond in kind.

Social Media

Physicians are people too, and may wish to participate with friends and family on social media such as Facebook. A physician may also wish to establish a professional presence online to let the community know about his/her expertise and availability. These two objectives should be kept completely apart.

The personal page should be kept strictly personal. Privacy settings should be used to assure that only family and friends, and not patients, have access to anything posted by the physician. The physician should also bear in mind that anything (s)he posts might become public, or even go viral.
The physician will wish to avoid posting any comments or materials that might cause the doctor to appear unprofessional. Patients and their treatment should never be discussed.

A professional or practice page should be understood as public service advertising and adhere to professional standards. A disclaimer should be displayed, advising viewers that information is provided for general education as a public service and that a qualified professional should be consulted for any health concerns.

Patients or potential patients should be advised that the social media page is not used to obtain medical attention; contact information can be provided for appropriate channels of communication. Omitting a patient's name from a clinical narrative, or face from a photograph, may not be sufficient to protect the patient's privacy, especially in smaller communities. Unless the physician has the patient's written permission, any discussion or depiction in which the patient could identify himself/herself should be avoided.

Resources

U.S. Department of Health and Human Resources, "Does the Security Rule allow for sending PHI (e-PHI) in an Email or over the Internet?" http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2006.html

Ofri, Daniel, M.D., 2011, "Should Your Doctor be on Facebook?" *New York Times* April 28, 2011. http://well.blogs.nytimes.com/2011/04/28/should-your-doctor-be-on-facebook/

Pho, Kevin, M.D. "How Doctors Can Use Facebook Responsibly?" April 28, 2008 http://www.kevinmd.com/blog/2011/04/doctors-facebook-responsibly.html

American Medical Association, Medical Ethics Opinion 9.124, "Professionalism in the Use of Social Media, June, 2011 http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9124.page

U.S. Department of Health and Human Services, Office of the Coordinator for Health Information Technology, "Guide to Privacy and Security of Electronic Health Information" Version 2.0, April, 2015 http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf