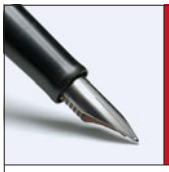


LETTER FROM THE EDITOR-IN-CHIEF

Security Risk Assessment: Protecting Patients and Practice

Securing protected health information (PHI) is a goal we all share. Collectively, however, we are relatively clueless about how to achieve this, largely because of the massive amount of technology that almost all of us have adopted. A simple understanding begins with the most basic categorization of the technology that we use to store, transfer, and manage PHI: Software and hardware.

Hardware includes all devices (desktops, laptops, routers, EKGs, and mobile devices) that store or are used to communicate and transfer PHI.

Software includes all programs used to manage PHI. Electronic Health Records and practice management software are the most obvious, but "bolt on" software increasingly is being adopted in the urgent care setting to assist with things like remote registration, patient flow, and patient satisfaction.

Inventorying all the software and hardware that interfaces with PHI is a good place to start. Again, including all mobile devices in this list is crucial because their portability creates significant risk of a PHI breach.

The next step is to diagram the human interaction with your technology collective and identify all the steps in the process. Below is an example:

1. Sign-on
2. Access/Permissions
3. Editing rights
4. Exchange of PHI
5. E-mail
6. Texting
7. Travel
8. Use of devices outside of practice setting
9. Access to EHR/PM software from remote locations and devices

The final step is to perform a "Security Risk Assessment" (SRA). An SRA is a great way to audit your practice to ensure compliance with HIPAA and HITECH. Breaches are subject to significant fines, exposing the practice and individual employees to considerable risk. Your best bet is prevention.

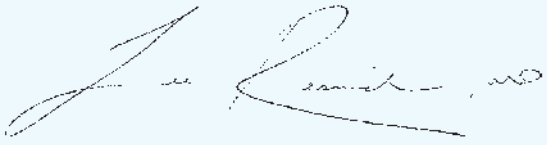
The steps and process for a Security Risk Assessment are outlined at www.healthit.gov.

What about "mitigation"? Many of the steps necessary to reduce your organization's security risk are self-explanatory and beyond the scope of this column. One area of risk mitigation that remains a challenge for all organizations is mobile security. Mobile security includes protection of all sensitive information that is stored on mobile devices like laptops and Smartphones. Lost or stolen mobile devices are by far the largest source of potential security breaches today, and for health care practices, which deal with sensitive patient data, the risk is even more acute. In addition to common-sense approaches, here's how technology can help protect your mobile devices:

Smartphones. The good news is that all data on most Smartphones and some tablets can be erased in the case of theft. On Android devices, download the Google Sync and/or the Google Device Policy and choose the "Remote Wipe" option to erase all files, email and other data in the device's internal storage and most files stored on the SD card. Users whose devices (including iPads) run on the Apple iOS can download the "Find My Phone" app and either "remote wipe" or "activation lock" their devices.

Laptops. The bad news is that wiping data from a laptop is far more difficult. Limiting access to the device is the best bet. In many cases, the simple password protection on most laptops is insufficient to prevent access to files, email, and other sensitive data. Emerging technology can help bridge the security gap: "Two factor authentication" is a method of security analogous to a "master lock" system. Access to devices requires a "second factor" access code (the Master Lock). This code is something only you could possibly know, or is something randomly chosen by the security vendor and sent to you via SMS text message. The technology can also be applied to most Smartphones. If your laptop is stolen, some of these programs can encrypt all of your files and make them unreadable to anyone without the second-factor identification.

Other emerging technologies for device protection include fingerprint and retinal identification, deemed "mostly" foolproof. But, if you've ever seen "Minority Report" with Tom Cruise, hang on to your eyeballs! Ouch! ■



Lee A. Resnick, MD, FAAFP
Editor-in-Chief
JUCM, The Journal of Urgent Care Medicine