

SALUMATICS

Source: Medscape Medical News © 2010 Medscape, LLC

Privacy Lapses Underscore Need to Keep Patient Data Off Portable Devices and Desktops

May 5, 2010 — So far, the real threat to privacy in the era of the electronic health record (EHR) is not a hacker, but someone who steals a desktop computer, laptop, external hard drive, thumb drive, or CD containing patient information.

Fortunately, the theft problem has an easy cure — never put patient data on these devices in the first place.

This imperative emerges from a running tally of major breaches in healthcare data security that is posted on the US Department of Health and Human Services (HHS) Web site by the Office of Civil Rights. Last fall, as a result of the American Recovery and Reinvestment Act, HHS began to require healthcare organizations to notify it of any privacy lapses involving 500 patients or more within 60 days. Incidents below this level must be reported on an annual basis.

As of April 30, the Office of Civil Rights listed 66 incidents at or above the 500-patient threshold involving hospitals, health insurers, state health agencies, and private practices. The number of patients affected ranged from 501 at the Alaska Department of Health and Social Services to 998,442 at Blue Cross Blue Shield of Tennessee. The Tennessee data disaster stemmed from stolen hard drives.

In all, theft of computers and data storage devices account for 56% of all the breaches, with stolen laptops leading the pack. Lost hardware accounted for another 6%. A few other hardware incidents involved neither theft nor loss. Another 24% of the breaches pertained to paper charts and hard-copy documents gone astray.

Only 2 privacy breaches starred a hacker, and only 3 hinged on email, and in 1 of those cases, the message was simply misdirected.

Web-Based EHR Systems Sidestep Theft Problem

For physicians using EHRs, preventing privacy breaches is not a matter of keeping computers and storage devices under lock and key but, rather, not storing data on them, according to healthcare computer consultant Rosemarie Nelson from Syracuse, New York. Achieving such good digital housekeeping depends on the kind of EHR system a physician uses, Nelson told Medscape Medical News.

Safeguarding data from hardware thieves is a relative snap for the growing number of physicians with EHR programs hosted on a remote computer and accessed via the Web. The party that hosts the program — an EHR vendor, a billing service, or a hospital — is called an application service provider, or ASP. With the ASP model, patient data as well as the EHR program typically reside on the remote computer, as opposed to a server in the physician's office.

"Doctors can access patient data anywhere in the world if they have a device with a Web browser," Nelson said about the ASP model. As a safeguard, they should configure the system so that no one in the practice can export patient data from the remote computer to a desktop computer, laptop, smartphone, thumb drive — anything.

"Thin Clients" and "PC Blades" Also Safeguard Data

Other physicians prefer that their EHR program and the patient files live inside an office server that is the hub of a traditional client-server network. Nelson said physicians can avoid thievable data on this kind of setup as well. Some practices, she said, have turned to the safety of "thin client" computing. A thin client is a small piece of hardware that connects a workstation monitor and keyboard to a back-office server. Unlike a regular desktop computer, a thin client lacks any kind of drive that would let it store data.

"You don't have to worry about theft this way," said Nelson.

Another variation on the thin theme is a so-called PC blade. With this technology, a computer user still sits at a workstation monitor, but the workstation has its own computer — or, rather, the components of a PC tower or box, such as a microprocessor, random-access memory, and hard drive. However, all these PC components sit on a back-office rack in an assemblage called a blade. What replaces the PC tower or box at the workstation is a dumbed-down piece of connective hardware with no data storage capacity.

Even without thin client or blade technology, Nelson said, a physician can keep all of his or her patient data safely on the network server by configuring the system — as with the ASP version — so that data cannot be saved on any device with storage capacity. For prudence's sake, the server should be kept in a lockable room or closet.

If a physician cannot download patient files with a client-server network, how can he or she work on patient charts with a laptop at home? The solution here, said Nelson, is virtual private network software that encrypts data transmitted over the Internet. This technology gives physicians the same experience as if they had an ASP-model EHR.

Physicians who insist on downloading patient charts on a portable computer should take the precaution of equipping it with password protection and encrypting the data on it. When stored data are encrypted, a medical organization is exempted from having to report the loss or theft of the device to HHS. Visit the HHS Web site for more information on the department's rules for reporting privacy breaches.

Consider Backing Up Data Online

One ritual in modern medicine is for a physician or office manager at day's end to take home a backup copy of clinical and business data in the form of a tape or a portable hard drive. Frequently, these backup devices do not return to the office — they get lost or stolen.

One alternative to toting around backup media is storing them every night in a fireproof vault in the office. Another alternative, which Rosemarie Nelson recommends, is backing up data via the Internet using a commercial data backup firm. Echoing the ASP model for EHRs, a copy of a practice's data resides in a remote computer.

"There's no physical transport of the data," Nelson said. "People need to exercise due diligence in shopping for a backup firm, but if it has banks for clients, that's secure," she said.

Media Contact:

Allan Magnacca
President and CEO
Salumatics
Office: 905-362-2230 ext 2231
Mobile: 416-727-0839
allan.magnacca@salumatics.com

© Salumatics and SaluVision are registered trademarks of Salumatics Inc. in Canada.