

BUSINESS

Smartphones blamed for increasing risk of health data breaches

Physicians need to focus on making sure their mobile devices are secure, experts say.

By **PAMELA LEWIS DOLAN**, amednews staff. *Posted Dec. 19, 2011.*

The number of physicians using smartphones has reached a near-saturation point. Meanwhile, the number of data breaches is going up.

Coincidence? Leading experts think not.

Recent reports by Manhattan Research have found more than 81% of physicians use a smartphone, up from 72% in 2010. Also on the rise have been data breaches, which, according to research released in December by Ponemon Institute, have risen 32% in the past year. Ponemon found that 96% of all health care organizations surveyed said they had experienced at least one data breach in the past two years.

The report did not specify the percentage of breaches from mobile devices. But it stated, "Widespread use of mobile devices is putting patient data at risk."

Larry Ponemon, PhD, chair and founder of Ponemon Institute, commenting on its first study of patient privacy and data security, said, "This year it seems the issue of mobile devices has ratcheted up, because the adoption rate of smartphones that are really smart, or tablet computers, seems to have increased significantly."

Ponemon said mobile devices create a security risk in two ways. Data can reside on the device and can be accessed. Also, the device can be a way of gaining access to data that reside on electronic medical record systems at the health care organizations. Plus, many note, smartphones' size makes them easier to lose than a laptop.

Either way, someone who finds a lost device -- or the thief who stole that device -- can gain valuable data if that phone is not secured.

Ponemon's study looked at only 72 health organizations. However, mobile device security is a primary concern throughout the health care field.

In her address to the attendees of the Third Annual mHealth Summit in Washington D.C., Kathleen Sebelius, secretary of the U.S. Dept. of Health and Human Services, noted that a large number of violations are caused by unencrypted devices becoming lost or stolen.

Analysts say mobile devices are like other new information technology in health care: A technology is introduced, and the rate of adoption outpaces efforts to ensure its security. Mobile devices probably got ahead of some people's ability to manage them adequately, said James Noga, chief information officer of Partners HealthCare in Boston.

Many hospitals are aiming to bridge that gap by improving security so any mobile device a physician uses may access their EMRs safely. Analysts say there are precautions physicians can take as well.

Adjusting to physicians' mobile use

Many hospitals have struggled initially with meeting the demand of physicians who wanted to use their mobile devices -- not those given out by hospitals -- to access the hospital's EMR system.

In an October member survey by the College of Healthcare Information Management Executives, 79% of health care organizations said that because of user demand, they approved mobile devices that could be used in the health organization's environment. However, that approval doesn't mean every device has secure access. In some cases, hospitals use mobile device management companies to provide third-party security for devices that otherwise would be considered unsecure.

And some hospitals make it very plain -- if their systems can't be used securely by a certain mobile device, then no access is granted. Lynn Vogel, PhD, chief information officer and vice president of University of Texas MD Anderson Cancer Center in Houston, said early versions of some smartphones aren't capable of being encrypted and secured properly, so physicians can't use them to connect with the hospital's data centers.

Some physicians haven't been happy with the hospital's decision not to support certain devices, he said. They must use a device that "we can manage institutionally and that we can handle in terms of encryption," he said. "We will not bend on this."

In exchange for hospital system access, physicians must decide whether they want their personal devices subjected to the same security processes as any other hospital information technology. For example, if a phone is reported lost to MD Anderson's IT department, it is remotely wiped of its data. Therefore whatever personal data is on the phone will be wiped along with the institutional data, Vogel said. Physicians must sign an agreement to that policy before they are granted access, he said.

Rick Kam, founder and president of the Portland, Ore.-based data consulting firm ID Experts, said physicians also should be aware that many institutions will confiscate the phone if it's needed to investigate a breach.

What physicians can do

Physicians can help, hospitals say, by making sure their phones are encrypted. Software is readily available that will encrypt smartphones and mobile devices. Encryption means that information is sent in non-readable form, and must be "unlocked" by a "key" on the device of the person wishing to view it.

The Ponemon study found only 23% of health care organizations use mobile device encryption. Encryption offers a safe harbor under privacy and security regulations under the Health Insurance Portability and Accountability Act for organizations and practices that have a lost device. If the device is encrypted, there are no reporting obligations, although many report the incidents anyway in the spirit of transparency.

Experts also recommend that physician practices set policies on mobile use, with attention paid to security measures, such as antivirus software and password protection.

"Security is not necessarily job No. 1 of the user," Ponemon said. Ponemon's survey found 49% of health organizations do nothing to protect mobile devices. Some experts believe that percentage is even higher for small practices.

"Small practices don't necessarily sit down and talk about this stuff," said Rosemarie Nelson, principal of the MGMA Health Care Consulting Group. They are busy taking care of patients and don't have information technology professionals thinking through these issues for them, like hospitals do, Nelson said. She noted that several medical societies, including the American Medical Association, have resources to help guide practices in mobile device security.

George "Buddy" Hickman, executive vice president and chief information officer at Albany (N.Y.) Medical Center, said quarterly training meetings have helped raise awareness among physicians there. At those meetings, stories are told of incidents, not just at Albany, but also at other organizations across the country. He said policy is reinforced at those meetings, and physicians and employees are told of consequences experienced by workers whose actions resulted in a breach.

"We help people understand that this is a serious part of our business," Hickman said.

ADDITIONAL INFORMATION:

What causes health data breaches

A study by the Ponemon Institute looked at the extent and cause of data breaches. Analysts say smartphones are contributing to a greater number of breaches, though numbers on smartphone-only breaches weren't compiled. Survey respondents could give more than one answer.

Cause	In 2010	In 2011
Lost or stolen computing device	41%	49%
Third-party problem	34%	46%
Unintentional employee action	45%	41%
Technical glitch	31%	33%
Criminal attack	21%	30%
Malicious insider	15%	14%
Intentional nonmalicious employee action	10%	9%

Source: "Second Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, December

Are hospitals guarding against mobile data breaches?

A study by Ponemon Institute found that nearly half of hospital systems aren't taking any steps at all to protect patient data contained on mobile devices. Survey respondents could give more than one answer.

Action	Percent of organizations
Don't do anything to protect mobile devices	49%
Have policies governing proper use of mobile devices	46%
Anti-virus products installed	25%
Encryption solutions installed	23%
Password or keypad locks	21%
Other	12%

Source: "Second Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, December

Copyright 2011 American Medical Association. All rights reserved.

RELATED CONTENT

- » [7 things to consider when choosing mobile devices](#) Column Aug. 29
- » [Older doctors embracing tablets faster than younger counterparts](#) July 18
- » [Health care embraces the iPad: Doctors jump on new technology](#) Feb. 7