BYOD in Healthcare Requires Extra HIPAA Precautions

[fa icon="calendar"] May 23, 2016 9:06:34 AM / by Michael Stone

Hospitals have differing policies when it comes to letting healthcare providers use their personal — or bring-your-own-device (BYOD) — mobile phones and other electronics to transmit and work with patients' protected health information (PHI).

Simply put, some allow it; some provide a device for just work, allowing IT personnel to make the device as secure as possible; and some take a hybrid approach, such as telling physicians which brand to buy but leaving the rest to them, according to the Emergency Care Research Institute.

Though the hospital-provided approach has obvious security perks (if it's strictly followed and the separate personal phone is never used for work), all three still carry the same basic dilemma: Could allowing doctors to use devices in the hospital, at home, at the coffee shop and everywhere else impact mobile data security and jeopardize HIPAA-protected patient data?

Going by the numbers, the short answer is overwhelmingly yes.

A search of the U.S Health and Human Services breach database shows that between the start of 2014 and today, 65 healthcare entities have had at least 500 individuals' protected health information potentially compromised by breaches of "other portable electronic devices," which are all things electronic — thumb drives, mobile phones, etc. — excluding desktops and laptops.

(The number 500 comes into play because if at least that many individuals are possibly affected by the breach, it's posted in the public database.)

Sixty-four of these 65 breaches (one doesn't include a number for individuals affected) resulted in a total of 2,618,627 people potentially having their information compromised.

The major risks that lead to such breaches, according to the U.S. Office of the National Coordinator for Health Information Technology, are: lost or stolen devices, viruses and malware that might lead to the phone being hacked, unintentional disclosures to unauthorized users, and using unsecured WiFi networks.

The office offers a list on ensuring information on BYOD devices doesn't fall — figuratively and literally — into the wrong hands. Because losing the physical device is the most prominent risk, here are three major points from literal sense:

1. **Maintain physical control of the device.** Seems obvious enough, right? But what easier way for a would-be attacker to get PHI than through this primary access point. Of the 65 aforementioned cases of portable devices, 28 were from theft solely, 15 from loss alone, two from loss and theft, and five from loss and other factors — so about 78.5 percent of the 65 cases involved theft or loss in some way.

   These numbers fall in line with the American Bar Association saying that theft of mobile phones is the most common HIPAA security breach.

   Besides establishing policies and disciplinary procedures, there isn't much a hospital can do for outside the workplace, but while the physicians are there, they could be given a locker, for example, to add extra security for the physical device.

2. **Use a password or other authentication.** If the phone is stolen, the first — and maybe best — line of defense is for it to remain on lockdown. Android and iOS phones have proven to be greatly difficult to login to without knowing the password, so even though the physician's BYOD phone is likely already password-equipped, the hospital could check and reinforce.

   Also, though Android phones send themselves back to factory settings by wiping everything after 30 failed password attempts, iOS phones do this (after 10 attempts) only if the setting is enabled by the user. This is a good idea, of course, for making sure all patient and other data is inaccessible from an attacker trying to get in through brute-force password guessing.

   And then there's always the extra security precaution of fingerprint (biometric) logins.

3. **Install and activate wiping and/or remote disabling.** This feature gives the owner the option to wipe the machine clean regardless of location. It can be done on both iOS and Android devices.

Read the do's and don'ts of securing mobile and BYOD users

Download Now

Topics: Healthcare

Written by Michael Stone

Michael Stone is a writer and photographer based in Gainesville, Florida, who has had his work published in several newspapers, magazines, and websites. He writes about a variety of topics, including technology and its impact on healthcare and education. He holds degrees in journalism and communications from the University of Florida and Middle Tennessee State University. You can read more about him on his website, www.MichaelStoneOnline.com.

emeia@iboss.com