Medical Staff Briefing

Require employees to perform mobile device security—or take it out of their hands

Gaps in mobile security remain a threat to your protected health information (PHI) and leave you vulnerable to HIPAA violations, so train and, if necessary, limit employee use to reduce the risk.

Mobile devices such as smartphones and tablets were once considered a risky proposition in the medical practice environment. But that ship has sailed: A 2018 Physician Practice survey showed nearly 76% of respondents use "mobile health (mHealth) in their practice on a weekly basis," and a 2015 Kantar Media survey found 84% of physicians use smartphones for work reasons. "Smartphones are quickly becoming a lifeline to many for case-related communication," says **Mark Mele,** vice president and director of sales of Casetabs in Los Angeles.

At the same time, a recent Verizon survey found that in the healthcare industry, 25% of users had "experienced a security breach involving mobile devices during the past year." This doesn't necessarily mean a HIPAA breach, but "any security incident that resulted in the loss of data or system downtime," according to Verizon. That's not entirely bad news—in fact, the previous year's Verizon survey found 35% of healthcare respondents reporting such incidents, so it's a marked improvement. But the numbers show the threat persists.

"I expect the trend will be going up as more users start to rely more on mobile devices," says **Richard Swaisgood,** director of cloud productivity and automation at Managed Solution in San Diego.

Don't fear the smartphone

There's nothing intrinsically wrong with letting your employees use their own devices on the job to access PHI. OCR specifically answers that question: "Health care providers, other covered entities and business associates may use mobile devices to access electronic protected health information (ePHI) in a cloud as long as appropriate physical, administrative and technical safeguards are in place. The HIPAA Rules do not endorse or require specific types of technology, but rather establish the standards for how covered entities and business associates may use or disclose ePHI through certain technology while protecting the security of the ePHI."

OCR also offers tips for mobile device use of PHI, including passwords, encryption, and remote wiping capabilities in case of security emergencies such as a lost phone containing easily accessed PHI.

Experts note that in the practice setting, mobile devices generally connect to cloud servers to access data. That may seem intuitively unsecure—the word "cloud" sounds insubstantial—but if the practice is using a virtual private network (VPN), it should be no problem: "VPN has a significant security layer shield for the cloud-based services," says **Jethro Lloyd,** CEO of iLAB Quality in Indianapolis. Cloud servers have their own security advantages, such as automated backups. Of course, you should perform basic security when using a cloud server, just as you do with your in-house network.

Watch for user error

A common error for mobile users carrying sensitive information is exposure to public WiFi, which "means exposure to malware, viruses, and other attacks," says Lloyd. If a device is improperly set up, it can join public or other networks without alerting the user, offering hackers a means of entry. And users have proven unreliable about restricting their own use; Verizon reports 81% of respondents "admitted using public Wi-Fi, even when many said doing so was prohibited by company policy."

This reflects a wider problem: Employees and providers don't always follow the rules you lay down for them. In fact, those who ignore security protocols tend to do it over and over.

One possible solution: whitelisting, or "limiting your ability to connect to the public WiFi," says **Doron Hetz,** senior vice president of engineering at Casamba in Los Angeles. This is like the whitelisting sometimes done in office systems, where web and email users are only allowed access to certain domains—only in this case, "you limit the IPs that can access your environment," says Hetz.

Wipeout!

Employees might be amenable to a whitelist because it would only present an inconvenience during work hours.

What may get employee pushback is a remote clean-and-wipe policy, which would give the company the ability "to wipe remotely without consent" the employee's device when a security breach occurs and it's recognized that the employee's device is tied to it, says Lloyd.

Fortunately, it's possible to encrypt your data in such a way that it prevents copying of data from the application to the rest of the phone, says Swaisgood, which "helps keep company data secure and allows for the quick removal of data once a breach has been discovered or the device is lost."

You may find these security features handy if an employee walks out the door. Say an administrative assistant leaves a practice with sensitive data on his phone, says **Joel Maloff,** chief compliance officer for Phone.com, which offers a HIPAA-compliant solution for mobile devices. "A text notification or recorded voice message left on [the admin's] mobile phone from a patient with whom he's worked for years may seem harmless, but these communications are considered [PHI]. If there is no segregation between [the admin's] phone and the PHI, there is a high probability that HIPAA laws will be broken."

Swaisgood also counsels regular remote examination of devices that access sensitive information for security vulnerabilities. "Cloud-based analytics allows for the learning of your users' usage patterns, allowing the discovery of breaches early on," he says. "An example would be, if a user starts accessing data they normally don't access or if a user starts mass deleting files"—that would be a red flag that something is going on, either with the user or a hacker that got into the user's account.

Tokens in your future?

Your options may expand in years and maybe even months to come: **Hans Reisgies,** co-founder of Sequent in Santa Clara, California, says he's working to extend the tokenization security services his company provides to financial companies and bring them to healthcare as well.

"Both payment processors and healthcare have a similar problem—data is spread across many ecosystem parties, such as websites, payment terminals, etc.," says Reisgies. "When sensitive data is exposed at that many endpoints, it creates a large area [vulnerable to] attack. Healthcare has this problem with the digitization of healthcare records—a whole bunch of patient data is spread all over their ecosystems at labs, clinics, insurers, etc."

Tokenization replaces sensitive material such as PHI with token data "that has more limited usability," Reisgies explains. The real data that the anonymized token stands in for is stored in "data vaults," dramatically decreasing the area of attack, and is swapped out when needed. Thus, if a hacker were to get into a dentist's records, "he may see how many root canals the patient had, but not much else, and can't see who the patient is."

Until then, keep your data encrypted and a close watch on your employees' mobile use.

Editor's Note: This article originally appeared in Part B News.