TechTarget | SearchHealthIT

E-guide

PRO+ Content

mHealth Security: Best Practices and Industry Trends

In this e-guide

In this e-guide:

mHealth, the use of mobile phones and other wireless technology in medical care, is taking the healthcare industry by storm. Physicians are increasingly using smartphones, tablets and other mobile devices to view and update patient records, fill prescriptions and even email patients, and companies are responding by creating thousands more healthcare apps.

There is no doubt that mHealth can positively impact patient care and engagement, but there are many security problems that IT professionals must solve.

In this e-guide, our experts discuss the pros and cons of mobile devices in healthcare, explain best practices, and suggest tools and techniques for improving your mHealth security. Also, discover why health IT professionals stand behind mobile despite all of the warning signs.

In this e-guide

Best practices for mobile healthcare security

Reda Chouffani, Biz Technology Solutions

Mobile healthcare security depends on a strong top-down approach that informs employees of all possible threats -- including physical theft and remote device hacks.

The flexibility in care workflows, improved productivity for practitioners, and timely access to data are encouraging many providers to continue to give patients mobile access to their health records. On the flipside, opening mobile access poses significant data security risks to IT departments.

When IT adopts a new bring your own device (BYOD) policy, it affords users the opportunity to use their mobile devices to gain access to health information. This challenges the IT department to keep users' data secure and maintain HIPAA compliance -- particularly when the devices in use are not owned by the hospital.

In this e-guide

Data breaches not only endanger patient's personal information, but may also subject an organization to criminal implications and monetary fines. In order to avoid data breaches, IT must ensure the implementation of strong healthcare mobile security practices.

Protect the devices

The security of mobile devices can also be compromised by loss and theft. It's nearly impossible to ensure a device won't fall into the wrong hands. Healthcare organizations must take precautionary steps to protect data in the event that a device goes missing. Some methods to accomplish this include remote wiping and locking, as well as tracking the device through GPS to locate and recover it.

Encrypt the data

Patient data that is accessed from mobile devices is likely stored remotely. The information is usually sent to smartphones or mobile devices from a server located in a secure facility, behind firewalls. Information that travels wirelessly and is stored within mobile devices can still pose a security risk if left unencrypted.

In this e-guide

It is a mobile healthcare security best practice to encrypt the sensitive health information while it's being transferred, as well as while it's at rest. This will help mitigate any leakage and offer strong data protection to ensure compliance.

Restrict and control access

Mobile devices must follow access control processes and procedures similar to restrictions seen within the world of desktops and laptops. This means only users with appropriate authorizations can gain access to protected data on mobile devices, and only IT has adequate tools to audit and manage all users' permissions.

Contain certain apps and data

With most healthcare professionals using their mobile devices for a mix of personal and business use, it's challenging for IT to implement restrictions without causing end users to feel locked out of their devices. It is critical that mHealth apps that capture patient data stay isolated and protected from other tools or apps within mobile devices to avoid putting patient data at risk.

In this e-guide

To solve this issue, many hospitals and Fortune 500 companies have implemented app and data containment. This is done by running mobile apps separately from all other apps to prevent sensitive data from being copied or penetrated. Creating this separation between personal data and healthcare data reassures IT that patient data can be protected with the right BYOD policy.

Use strong policies and education

One of the best methods to improve the security of sensitive data within mobile devices is through user education. While users will have the best intentions at heart, implementing clear policies and procedures that define what can and can't be done on the devices is the surest way to avoid any gray areas. Some of the common requirements applied to accessing enterprise networks and health information are:

- The use of a passcode to access information on the device
- The use of application containment for all enterprise or health apps
- The IT department is notified when a device is lost or stolen
- Denying the sideloading of apps and device jailbreaking

In this e-guide

- Unauthorized users are restricted from accessing a device while a healthcare app is in use

Failure to implement some of these processes can put patients' health information at risk.

Implementation of mobile protection tools

It is a common practice for IT to roll out antivirus and antimalware tools on employees' desktops. Unfortunately, with the increasing number of infections targeted at mobile devices, IT must recommend or even require end users to deploy tools to protect mobile devices against viruses and malware. An IT department can leverage a mobile device management platform to monitor and report any infections or risks affecting compromised mobile devices.

Install only trusted mobile apps

Not all available apps offer guaranteed data encryption. Vendors like Apple, Google and Microsoft do not validate or look for data encryption. This leaves IT solely responsible to work with app developers to ensure data encryption is available and enabled.

In this e-guide

End users are continuously purchasing new devices and using new platforms and apps within the healthcare space to access protected health information. It is a challenge for IT departments to keep up with these changes and offer end users the flexibility to use their mobile devices while still ensuring all of their data is protected. With the selection of a robust mobile device management platform, and deployment of many of the highlighted best practices, it can be possible to secure health data on mobile devices.

Next article

In this e-guide

Despite risks, healthcare IT professionals stick with mobile

Kristen Lee, searchHealthIT News Writer

When it comes to mobile security, the odds seem stacked against healthcare organizations. Although the mood surrounding mobile among healthcare IT professionals ranges from cautious to downright terrified, they all acknowledge that the use of mobile devices will only increase despite the risks.

Healthcare organizations often lack the tools, resources and money needed to fully protect themselves against breaches, and hackers have strong incentives to steal patients' medical records.

For example, patient records can go for $20 to $50 each on the black market, and a complete patient record -- including the patient's driver's license, health insurance information and other sensitive data -- can be worth more than $500, according to a report by the Institute for Health Technology Transformation. If a healthcare organization has a security breach and hackers swipe 1,000 complete patient records, they could potentially fetch $500,000.

In this e-guide

"It's basically a treasure trove of information that these people want to get access to," Cletis Earle, vice president and CIO at St. Luke's Cornwall Hospital in Newburgh, N.Y., said.

Cletis Earle

In comparison, credit card information can sell for just $1 and personally identifiable information can sell for $10 to $20.

"It's impossible to cover it all. You can cover a lot of it and the majority of it, but there's still things coming up ... that we're not aware of, and a new threat is going to occur or a new vulnerability is going to occur to the organization," Earle said. In fact, he added, "you probably are already breached."

However, experts say, in general the risks have not deterred the medical community or healthcare IT teams from adopting mobile.

Kirk Nahra

This is partly due to the fact that the risk of a cyberattack has been around long before mobility came into everyday prominence. For example, the Anthem breach -- in which hackers got into a database by running a computer program under a staffer's personal identifier -- did not stem from mobile devices, Earle points out.

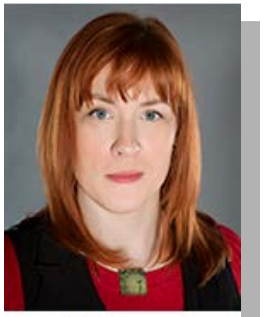
"[Healthcare IT professionals are not] necessarily viewing mobile as anything different or harder or riskier than anything else," Kirk Nahra, an attorney at Wiley Rein LLP who specializes in privacy and information

security who recently spoke about these issues at the HITRUST 2015 conference, said.

And the implications for mobile endeavors in the healthcare space-- such as telehealth, value-based care and increased patient engagement -- cannot be ignored.

"Our goal is to take care of patients that are going to be outside the four walls of the hospital. The hospital is going to be a different care continuum ... Healthcare is definitely becoming more entrenched in the community and the only way of dealing with things in the community is using that mobile strategy," Earle said. "It is definitively going to be the norm."

Healthcare IT feels the pressure


Lysa Myers

With HIPAA regulations, meaningful use requirements and the knowledge that a breach is inevitable, healthcare IT teams are under a lot of pressure -- especially with five different agencies conducting audits and some healthcare organizations not passing those reviews, said Lysa Myers, a security researcher at ESET, an IT security company.

Although IT teams take mobile security into consideration, the fact that there are so many other areas within a healthcare organization vulnerable

In this e-guide

to attack means that mobile is not the sole focus. Instead, healthcare IT professionals tend to look at the bigger picture.

"Yes, we are absolutely terrified," Earle said. "You may already be attacked, you may be under attack, but how and what are you putting in place as a CIO or as an IT executive [so that you can] recover from that breach and from that attack? It's pivotal to put the plans in place to say how you're going to recover."

A number of healthcare CIOs told SearchHealthIT at HIMSS 2015 in Chicago that data security is a top priority.

"We're going to triple down on data security," Marc Probst, vice president and CIO at Intermountain Healthcare, said at HIMSS 2015."It's of paramount importance and none of the rest is really going to be useful if we can't secure and assure our patients that the data will be private."

> **We're going to triple down on data security.**
>
> **Marc Probst**
> vice president and CIO, Intermountain Healthcare

Next article

In this e-guide

Tools and techniques to improve mobile device security in healthcare

Nari Kannan, searchHealthIT Contributor

Clinicians are clamoring to use their iPads, but they must be secured. This tip examines eight trends in mobile device security that help keep healthcare data safe and secure.

According to a new report by Manhattan Research, fully two-thirds of physicians in the U.S. will be using Apple iPads for professional purposes by 2013. A similar study in Europe showed that about 26% of physicians owned and used an iPad. Healthcare workers are using mobiles and tablet computers for various purposes such as looking up drug interactions, other medical reference material and, in some cases, electronic medical records of patients.

That brings to the forefront the issue of security of transmission and storage (even if temporary) of personal health information on these mobile devices. Privacy mandates like the Health Information Portability and Accountability Act (HIPAA) also heighten anxiety about storage and use of personal medical information.

In this e-guide

Healthcare workers have been clamoring for some time to bring their own mobiles and tablet computers into work, expecting to access work-related applications on them. Consequently, healthcare IT has been setting up bring your own device (BYOD) policies considering the variety in device preferences of the workers. This way they can exercise some level of control over security and privacy of healthcare data.

Current trends in mobile security promise a number of different ways in which security and privacy of health data can be addressed effectively. Some of these are:

Desktop as a Service (DaaS) usage on mobiles: Recently Dell rolled out its Desktop as a Service (DaaS) offering. On mobiles and tablets, this allows desktop environments to run virtually and access applications in their native forms (like a Windows desktop or a Macintosh). This is as if a virtual desktop resides inside the mobile device. The biggest security win in this approach is that no additional security is needed. If the owner of the mobile device is no longer with the company, this access is disabled. All applications and data reside in internal servers and no data is present locally on the mobile. Companies can adopt BYOD policies easily since the applications are not on the mobile devices, which means a larger variety of devices can be supported.

In this e-guide

Access control lists: Access control lists (ACLs), also known as role-based logins, control which users, using which mobiles can access an application. They can also have finer control over what data within that application they can access and what they can do with it (for example, read, read/write or read/write/delete). Fine-grained control using ACLs allows IT departments to tailor security policies to different types of users and enforce them diligently.

Encrypted data transmission: Virtualized desktop environments may already have 128-bit, built-in encryption of any communication, including data to and from mobiles and tablet computers. If native apps are developed for mobiles, they may need to do this when they communicate with servers.

Double encryption: When you use strong 128-bit encrypted transmission and storage of data on mobile devices, use of a Virtual Private Network (VPN) connection enables the encryption of already encrypted transmissions. This provides double encryption, a strong way of protecting data and transmissions.

Remote wipes and auto-locks: Native apps on mobiles invariably use local storage, even if only for temporary download of healthcare data. Mobile device storage may need to be remotely wiped clean when the device is switched off. When mobile devices are lost, misplaced or stolen, the same remote wipe capability may be needed. Most mobile devices support auto-locking the device remotely, if lost, misplaced, or stolen.

In this e-guide

When located again, they also require long pass codes to reactivate, providing one more layer of security. There are commercial mobile device management software packages that can register devices and do these remote wipes when warranted.

Mobile ID authentication mechanisms: Additional authentication mechanisms may need to be implemented with something like real mobile device identification (unique ID of a smartphone or a tablet) and a company-assigned machine ID that is assigned to say, a clinician. Only with both these IDs will the mobile device be allowed to access the network. This is an additional security precaution to authenticate physical mobile devices.

Isolated special subnets for mobiles: Mobile devices like smartphones and tablet computers may need isolated special subnets, meant only for them. By having a separate subnet, mobile device usage can be logged for audit and unauthorized access detected. Subnets can also ensure better bandwidth Quality of Service (QoS) for mobile devices. Desktops and laptops may hog a network's bandwidth if they share the same network with mobiles and tablet devices.

Signal range control: By making the wireless signal to the mobiles reachable only within the premises of the healthcare setting -- such as within a hospital or clinic -- or only at home through VPN, security and privacy can be enforced by restricting where applications are accessed

from. This may not work very well if employees need to travel on business, but for healthcare applications that don't involve travel, this will work well.

Increasing use of mobile devices in healthcare settings brings with it many security problems. Depending upon how the applications are accessed, through a virtual desktop or as native apps, those problems will vary. However, trends in mobile device security promise many methods to address these issues. By matching the needs of a particular healthcare setting to these tools and techniques, security and privacy can be effectively ensured. A number of commercially available mobile management software solutions can help healthcare IT pros create and administer these policies.

Next article

In this e-guide

Mobile devices in healthcare come with pros and cons

Trevor Strome, Winnipeg Regional Health Authority Emergency Program

Nearly every physician uses a mobile device during business hours. Providers are adjusting to this trend by building better wireless infrastructures.

The tablet and smartphone are becoming nearly as ubiquitous in healthcare as the stethoscope. One survey in 2013 discovered that 86% of physicians used smartphones, and more than half of providers used tablets, in their day-to-day clinical activities. Those numbers are certainly greater now. The survey estimated that by 2014, more than 90% of physicians would have adopted smartphones and nearly that same number would be using tablets.

One reason for the popularity of mobile devices in healthcare is convenience. In one handheld device, providers can access patient information, research medical literature, and securely communicate with patients and colleagues, among other tasks. Another factor behind the use of mobile devices is the availability of targeted apps. One estimate pegged the number of clinical applications for mobile devices at 95,000.

In this e-guide

The use of mobile devices in healthcare is driving the deployment of wireless infrastructure within healthcare organizations. According to a report by ABI Research, wireless technology in healthcare is flourishing because of "the healthcare industry's need for staff mobility, transfer of digital records, standardized administration of medications and improved asset management."

The mobility and convenience of devices such as smartphones and tablets, coupled with the number of available clinical applications, can lead to benefits for healthcare providers. According to the book *Wi-Fi Enabled Healthcare*, there are several aspects of healthcare that benefit from the wireless capabilities.

- Workflow: Wi-Fi allows for apps to provide information entry at the point of care and quick access to patient information, such as bedside registration, diagnostics, and patient and staff tracking.
- Communication: With Wi-Fi, mobile devices can facilitate secure, real-time communications between healthcare providers and patients.
- Emergency treatment: Information from emergency services can be relayed while en route or even while first responders are in the patient's home.

In this e-guide

- Asset management: The location and status of equipment can now be relayed to make it easier to locate items.
- Data access: Applications that use Wi-Fi on mobile devices facilitate the collection, analysis and sharing of critical patient data -- including data on EHRs.

In addition to tablets and smartphones, other types of medical devices and applications contribute to the need for continued deployment of Wi-Fi at healthcare facilities. According to the Wi-Fi Alliance, some of these additional devices and applications include "infusion pumps, oxygen monitoring devices and smart beds, alongside mission-critical information applications such as access to electronic medical records ... and real-time access to X-rays and MRI scans." Wi-Fi also supports the provisioning of high-quality telehealth to geographically remote or underserved areas, and to a growing extent, within healthcare facilities themselves.

Wi-Fi in healthcare is also growing due to the rising demand for mobile access to clinical and administrative information. According to an estimate by ABI Research, the market for healthcare-related Wi-Fi services is expected to reach approximately $1.34 billion by 2016. This number will climb as new uses of Wi-Fi in healthcare, such as voice over Wi-Fi and real-time location systems, expand alongside smartphone and tablet use.

In this e-guide

According to the ABI Research report, existing Wi-Fi applications are expected to be joined by "a new generation of medical body area networks (MBANs), which ... take advantage of Wi-Fi connectivity to support mobile monitoring capability." Nearly 30 million MBAN devices are projected to be shipped annually by 2016.

There is no doubt Wi-Fi is transforming the way information is accessed, collected and used within healthcare organizations by both clinicians and administrators. Wi-Fi is even improving the patient experience by permitting easy, cost-effective access to the Internet using their own smartphones and tablets within hospitals. This communications portal that connects friends and family can go a long way to easing what is sometimes a lonely and stressful time for patients. By improving workflows and increasing the speed with which physicians can access critical information, Wi-Fi can play an important role in improving the efficiency of care provided by hospitals.

Next Article

In this e-guide

Healthcare workers breaking free from offices

Reda Chouffani, Biz Technology Solutions

Mobile devices -- supported by a vast application marketplace and ease of use -- have enabled remote workers to perform all of their tasks outside of a traditional office setting. This has only been fully realized in some non-healthcare settings. Healthcare employees deal with a different set of circumstances because care workflows typically require showing up at the hospital or doctor's office.

But they too can leverage many of mobile devices' capabilities to become more efficient.

In most traditional business settings, staffers need on-demand access to email, a dedicated voice line, as well as a desktop computer. These are reasons why staff members are tied down to a cubicle. A growing number of hospitals recognize that employees should be given the flexibility to be able to do most of these things while on the go.

Hospitals owned by Carolina Health Systems -- current users of Microsoft Lync -- are evaluating the voice capabilities of the platform to see what it

In this e-guide

can provide its employees. Lync is a platform that aims to enable full voice capabilities for users through a softphone that comes with the program.

Lync is only one of the products that can make a case for mobile health employees working remotely. There are other enhancements and capabilities available in today's mobile devices that are enabling more healthcare employees to be fully functional outside of the office.

Robust apps and mobile devices

Hospital users can leverage the increasing compute power of today's mobile devices and apps to gain access to digital content within the health system. In cases where hospital data systems don't have native apps to run on phones and tablets, IT departments can open up those systems to mobile devices via virtualization. These mirror the same functionality their traditional desktop counterparts offer.

Communication capabilities

Beyond emails, mobile devices and tablets are equipped to handle applications such as Microsoft Lync and other software that fully supports voice capabilities. Long were the days when your extension was only

available at your desk. Now, end users can have their extension ring on their mobile device wherever they have Internet connectivity.

Improved collaboration

One of the arguments against staff working remotely or being constantly on the go is a resulting lack of interaction or collaboration. While mobile devices can never replace face-to-face interactions, through a combination of apps, they can allow physicians, nurses and patients to connect and access medical records from anywhere.

Hospitals can offer mobile workers the tools and functionality to help increase their productivity. Unfortunately, as more employees choose to work remotely and some others bring their work home with them at the end of the day, hospitals are burdened with heavier mobile security and data protection loads. Healthcare CIOs and IT teams must be fully aware of these risks and be able to address them with the right policies and tools.

Next Article

In this e-guide

Providers work for security in healthcare, lock down mobile devices

Shaun Sutner, searchHealthIT News and Features Writer

With mobile devices proliferating -- and security in healthcare lacking -- providers are ramping up efforts to better safeguard devices and related apps.

When Care New England, one of Rhode Island's largest healthcare systems, installed a patient-rounds app on the smartphones physicians use to link to ambulatory clinic EHRs, it was only after a month of rigorous in-house testing of the app's security.

Concerns about the lack of security in healthcare apps -- which are multiplying as rapidly as the mobile devices that host them -- is only one of the problems vexing healthcare CISOs and CIOs as they confront the mass movement toward mobility.

Chris Logan, CISO of Care New England, said he worries constantly about potential breaches of the healthcare system's network, connected medical devices and mobile platforms, though he hasn't seen a loss or theft of protected health information (PHI) from a smartphone or tablet.

Yet.

"But I guarantee you it's going to happen," Logan said. "It's not a matter of if it's going to happen, but when."

In addition to app security testing, Care New England has set up an internal "app store," from which about a dozen security-vetted apps are available to doctors, clinicians and other staff.

Report critiques mobile security

As it happens, Care New England's preventive measures are key recommendations in a February 2015 report on *The State of Mobile Application Insecurity* by the Ponemon Institute, an independent privacy think tank. The study was sponsored by IBM, which sells an array of data security systems into healthcare and other industries.

The report, which relied heavily on respondents in healthcare among the 640 people surveyed, came up with these main findings:

- The "rush to release" results in mobile apps that can contain vulnerabilities.
- Mobile apps are rarely tested in production, and if they are tested, it is only in development or post-development.

In this e-guide

- The number of malware-infected mobile apps and devices is increasing, and few organizations are able to prevent their use.
- Not enough money is spent on security as part of mobile app development.
- There is a widespread lack of security professionals in enterprises.
- Most employees are heavy users of apps, but they don't have policies that govern this use.

The Ponemon report and other recent studies have looked at issues facing mobile security in healthcare and have noted the historic evolution from desktop computers to laptops and now to a massive influx of handheld mobile devices, in the work world and among consumers.

"It's kind of like a runaway freight train," said Larry Ponemon, founder and CEO of the institute. "And the attitude in the healthcare industry is sort of go with the flow and pray your security is adequate."

By comparison, as cyberattacks on corporations and healthcare systems have mushroomed over the last year or two, organizations have quickly ramped up security efforts to combat that problem, adopting such strategies as virtualization, encryption and multi-factor authentication.

In this e-guide

Mac McMillan, co-founder and CEO of Austin-based consulting firm CynergisTek, said mobile security in healthcare is still in its infancy. At the same time, he said, the soaring popularity of wearable health technology devices for consumers, such as fitness trackers, as well as more sophisticated medical wearables, compounds the security challenge.

"It's still very much chaotic," McMillan said. "But the momentum behind it is tremendous."

McMillan advocates mobile device management (MDM) strategies for providers coupled with rigorous employee training and technologies such as "containerization," in which provider organization apps and network access are locked up in encrypted icons on mobile screens.

Journal article questions privacy of app data

Three eminent physician-researchers -- Stephen Steinhubl, M.D., Evan Muse, M.D., and Eric Topol, M.D., author of the influential book about patient-directed healthcare, *The Patient Will See You Now* -- have issued a similar stern warning about the security, privacy and safety risks accompanying the sudden explosion of mobile technology in healthcare.

In this e-guide

In an April 15 article in *Science Translational Medicine*, a publication of the American Association for the Advancement of Science, Steinhubl, Muse and Topol note that the Federal Trade Commission recently tested 12 mobile fitness apps and found that the apps sent consumer data to 76 different third-party companies.

The data included phones' unique device identifiers and personal information about owners' running routes and eating and sleeping patterns. Perhaps more worrisome, the authors reported, a 2014 analysis by the Privacy Rights Clearinghouse found that nearly half of the 43 apps in the study collected high-risk financial information and personal health and identifying information. More than half of the apps shared the data with third-party analytical services.

> **The attitude in the healthcare industry is sort of go with the flow and pray your security is adequate.**
>
> **Larry Ponemon**
> founder and CEO, Ponemon Institute

"In the era of big data, it is critical that the terms of ownership of personal data, most especially medical data, be unambiguously stated -- not buried in the universally unread and then accepted terms of use agreements -- with users required to explicitly consent whenever their data are sold or transmitted to others," the authors warn. "It is unlikely that this will occur without new laws and regulatory oversight."

In this e-guide

Technology limits user interaction with corporate data

In the absence of such governmental oversight -- and to control the bring your own device (BYOD) culture that pervades healthcare and is likely to persist indefinitely -- many providers turn to tech giants such as IBM and Dell to provide mobile security. Both companies have gone into the security business in recent years by acquiring smaller security companies.

Smaller independent security vendors such as Bottomline Technologies are also seeing brisk business. Bottomline recently signed a multi-year deal with Cedars-Sinai Medical Center in Los Angeles to run the Portsmouth, N.H., company's Healthcare Data Security and Privacy system to track users' behavior on the hospital network using analytics, forensics and real-time monitoring.

Fiberlink Communications, an IBM subsidiary, has had success with its cloud-based, MaaS360 line, an MDM containerization system for small and medium-sized enterprises.

For a subscription fee, customers, including healthcare providers, get encrypted container icons, each with its own unique PIN, installed on their employees' tablets and smartphones. Updates are delivered automatically by way of the cloud.

In this e-guide

Employees can still use their own apps, but they are walled off securely from the container, said Chuck Brown, director of product management for Fiberlink. In the opposite strategy, organizations handle their own mobile security by giving users secured, corporate-owned devices on which employees can only use approved apps.

"The data is protected inside the container. This plays well into a BYOD situation," Brown said. "Some people don't like 'Big Brother' looking over their shoulder."

One Dell user, Green Clinic, a 50-physician practice in northern Louisiana, uses Dell SecureWorks' cloud-based systems to secure its doctors' iPhones and iPads.

Meanwhile, the clinic's mobile users are walled off from the practice's EHR from Greenway Health LLC, so they can't touch PHI on the EHR. Instead, they communicate through Dell SecureWorks' PocketCloud, which puts a mini version of the EHR on their mobile devices, then wipes it clean when the doctors log off.

"We're pretty strict about not leaving PHI on our devices," said Jason Thomas, Green Clinic's CIO and security director.

Next Article

In this e-guide

Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers – a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia