MANAGING IPADS IN THE HOSPITAL

Doctors love iPads—and whether IT departments like it or not, they are bringing the devices into the hospital. Fortunately, a combination of common sense and general best practices will address device management, network infrastructure and data security concerns.

LOVE THE IPAD

THE HEALTH CARE industry in general is not widely regarded as a willing adopter of information technology. Anyone who has gone to the doctor and filled out a multi-page form that lists dozens of potential illness symptoms can attest to this. However, when the Apple Inc. iPad took the mobile device market by storm two years ago, physicians bought the tablets in droves.

It didn't take long for physicians in particular, and health care in general, to see the potential the device held. For years, the industry sought a tablet that could fit in a physician's white coat pocket, pull up patient data at a moment's notice and, critically, not interfere with the patient encounter.

Although the iPad isn't perfect—physicians and vendors alike have cited concerns regarding its durability, battery life and ergonomics—its sheer ubiquity has made it the tablet of choice for health care. Its ability to let physicians answer key questions about a patient's condition or treatment options while outside hospital walls has certainly helped, too. As the cliché goes, every single U.S. physician has children who play soccer and can expect the game to be interrupted with an urgent request to look at a patient chart.

IT departments in health care now face the challenge of accommodating the bring your own device (BYOD) phenomenon, which brings with it concerns about device management, network infrastructure and, critically, data security.

All agree that the extra effort to support the iPad beats the alternative of turning a blind eye, letting users go rogue and facing the—often costly—consequences of a data breach or broken electronic health record (EHR) system at a later date.

Our staff and contributing writers have worked hard to address as many iPad implementation headaches as they can. If this e-zine leaves any questions unanswered, email me at beastwood@techtarget.com or visit our Health IT Exchange community site to ask your question to health IT experts and peers. ■

BRIAN EASTWOOD
Site editor, SearchHealthIT.com

CHAPTER 1

PREPARING NETWORK INFRASTRUCTURE FOR HOSPITAL IPAD USE

Hospital network infrastructure usually supports both wired and wireless access. When staff start using iPads to access patient data, networks must meet additional requirements. **BY NARI KANNAN**

THE Ottawa (Ontario) Hospital is the largest acute care hospital in Canada, with 1,163 beds and 11,967 staff members, among them 1,159 attending physicians and 3,886 registered nurses. The hospital announced in December that it will use Aruba Networks Inc.'s WiFi Mobile Virtual Enterprise (MOVE) system to connect 3,000 Apple devices—including iPads, iPhones and iPod Touch units—at the medical facility. The MOVE system serves wired laptops and desktops as well as wireless devices. The hospital needed doctors and nurses to be able to walk around the hospital with iPads so they could access the electronic health record (EHR) and computerized physician order entry (CPOE) applications.

Meanwhile, Children's Hospital Central California plans to deploy iPads in a different way. The hospital, one of the 10 largest pediatric hospitals in the country, is rolling out VMware Inc.'s VMware View Client on iPads so clinicians and staff can stay connected to virtual Windows desktops anywhere in the building. The VMware View client is designed to emulate the multi-touch user interface of the iPad, but the applications are the same as what one would access on a desktop in building.

Although the above case studies show that the underlying software architecture of iPad deployments can differ, hospital network architecture

nonetheless needs to meet some basic requirements. The following requirements are common for all hospital iPad use cases:

- **Unified wired/wireless access.** Many hospitals may be already using desktops or laptops for doctors and nurses to access EHR, CPOE and other applications. Hospital iPad use for these apps may not be far behind. Laptops could be used in wired mode at someone's office, but users may need wireless access if they are in a conference room in the hospital. The same network infrastructure needs to support both wired and wireless access seamlessly.

- **Policy redeployment for mobile devices.** Use of applications such as Epocrates is already widespread in many hospitals with iPhones and iPods. For these, and other basic applications such as email, hospitals may already be providing basic wireless network access, with some minimal secure access. Until now, mobile devices may not have had access to hospital applications.

- **Additional network access points.** Hospitals may vary in size from a few hundred thousand square feet to campuses with multiple buildings running into millions of square feet. Pilot deployments and phased rollouts in select areas of the hospital are pretty common. Usage may increase over time. Increasing network traffic needs monitoring and modular scaling of additional network access points as necessary.

- **Network load and quality of service (QoS) balancing.** When the same network infrastructure serves wired and wireless devices, those different devices may need different Quality of Service (QoS) levels. It may be necessary to monitor QoS on wireless devices at various locations within the hospital and to make adjustments, both when applications requiring vastly different bandwidth are in use—text messaging vs. downloading and viewing an X-ray—and when mobile device users move from areas of high to low connectivity within the building.

- **Device fingerprinting.** On the network side, device fingerprinting, which assesses a device's hardware and software settings, can recognize whether a device that needs a connection is a mobile device or a wired device. This information may be needed for appropriately ensuring QoS levels for all devices.

- **Authentication services.** In addition, devices may need to be registered with the network infrastructure to ensure that a mobile device is really the mobile device it says it is.

Mobile device authentication services must prevent unauthorized access to the network, to applications and, most importantly, to medical data. HIPAA privacy violations are penalized severely.

- **Remote wipe capability.** Many hospital iPad deployments provide access to applications and data only within the hospital campus. In addition, they do not allow local persistent storage of medical data on the iPad. Hospital network infrastructure may need behind-the-scenes data streaming—that way, when an iPad is on, data is available, when the iPad is switched off, data can be remotely wiped from the iPad.

- **Multicast video conferencing capability.** The iPad's built-in camera, combined with mobile video conferencing platforms from vendors such as Polycom Inc. and Vidyo Inc., makes it a prime candidate for videoconferencing and other telemedicine initiatives. To make this possible, network infrastructure should support multicast communication between one sender and several recipients.

- **Patient video monitoring support.** Video applications, especially on mobile devices like the iPad, are bandwidth intensive. This includes videoconferencing as well as video monitoring, which hospital personnel can use to keep an eye on patients from afar. To accommodate such applications, network infrastructure may need additional bandwidth.

- **Uninterrupted power.** As hospital iPad use becomes increasingly mission critical, especially in situations such as a power failure, providing uninterrupted power for the network gains importance.

- **Network monitoring system and logging.** To support hospital iPad use, network infrastructure needs comprehensive network monitoring and logging that records the exact device, the applications and the data it accesses, and the timestamps. While applications may have their own logging, tracking access from specific iPads may be needed for additional security and audit purposes.

Extending access with iPad EHR systems and other hospital applications introduce additional network infrastructure requirements. However, once these requirements are addressed systematically, hospitals can see successful iPad deployments. Caregiver and patient mobility are enhanced, which leads to better patient outcomes, efficiency and effectiveness. ■

Nari Kannan is the Chief Executive Officer of appsparq Inc., a Louisville, Kentucky-based mobile applications consulting company. He has over 20 years of experience in information technology.

EXPERTS DEBATE MERITS OF VIRTUALIZED VS. NATIVE IPAD EHR

Native apps and virtualization both have their tradeoffs for iPad EHR implementation, but health IT leaders agree: The tablet is here to stay in hospitals. **BY DON FLUCKINGER**

AMONG PHYSICIANS AND nurses, iPad adoption is expanding at a much faster rate than in the general consumer population—and they want their electronic health records system to run on it. That leaves CIOs with a dilemma when it comes to hospital iPad EHR implementation: Run a native app or a desktop virtualized to the iPad?

Both have their tradeoffs. Virtualized environments offer unparalleled security—and by extension, HIPAA compliance—at the expense of speed and features tailored to the iPad and iOS operating system's touch screen.

Native iPad EHR systems, on the other hand, dovetail better with the iPad's design, with scrolling, page-turning and other features iPad die-hards swear boost their productivity. However, these apps can also pose risks when an iPad is lost or stolen and therefore require more security safeguards. Native apps also may require in-house development or customization resources that many hospitals cannot afford.

Overall, if you can get employee buy-in for an iPad EHR implementation, said Dale Potter, senior vice president and CIO at Ottawa Hospital, it is quite economical. "These devices are six hundred bucks," Potter said. "Some medical equipment these physicians carry around—[such as] a stethoscope—can cost you much more than that."

VIRTUALIZATION IN INDIANA EHR IMPLEMENTATION

Before the "virtualization or native" decision can be made, Deaconess Health System CIO Todd Richardson said, a hospital has to decide if it will purchase iPads or let employees bring in their personal devices to use on the network. He took the latter approach for the six hospitals in his system, which serves western Kentucky, southern Indiana and southeastern Illinois.

His organization adopted the view that tablets, like cell phones, are a personal investment—everyone who truly wants one already has one. Not only does that kind of thinking eliminate the capital outlay and need to track iPads throughout the enterprise. It also saves IT staff from policing devices for personal data and apps such as contacts and music. Furthermore, the policy prevents the "arms race" between physicians lobbying IT staff for upgrades when faster, larger-capacity iPads come to market—users either upgrade themselves or they don't.

"As a CIO, it makes me sleep easier at night knowing it's a pain. I don't have to deal with, quite frankly," Richardson said. "And they're going to take better care of it."

That said, there's no one right way and one wrong way to do an iPad EHR implementation, said Richardson, who chose to use Citrix Systems Inc. to virtualize the hospital's existing Epic Systems Inc. EHR system. "Different health care systems have different cultures, and different ways of doing things. What works in one spot clearly does not work from Santa Fe to Evansville to Waterloo, Iowa."

WITH THE VIRTUALIZED EHR IMPLEMENTATION, NO PATIENT DATA IS STORED ON THE IPADS. THIS GREATLY SIMPLIFIES HIPAA COMPLIANCE.

With the virtualized EHR implementation, no patient data is stored on the iPads. This greatly simplifies HIPAA compliance. Richardson said the difficult challenge in getting the system to work was creating wireless connectivity throughout their facilities, which include lead-lined buildings that required creative positioning of access points so physicians would not drop off the network. It became especially thorny in difficult spaces such as stairwells. After that came the issues of securing the wireless network and giving physicians priority bandwidth.

Although the transition has not been seamless, Richardson said phy-

sician affinity to the iPad is so great that they will take on the learning curve.

"We had the experience of a neurosurgeon calling and screaming because he couldn't connect from Owensboro [Ky.] on his iPad to check orders and things," he said, sheepishly. "When you've got a neurosurgeon screaming at you that [he] can't connect through [his] iPad, you've won the war—and now the battle is figuring out why it's not connected."

CANADIANS ROLL THEIR OWN IPAD EHR

Potter, who is CIO of the largest academic medical center in Canada, decided that the iPad's touch screen operating system offered such great efficiencies—and at great savings compared to traditional computers—that he bought into it, literally. So far, he's purchased thousands of the devices for his clinicians and hired 124 software developers to write apps porting his Oasis Healthware EHR system to the iPad.

That decision came after he witnessed several vendor demos of what looked to him like poor implementations of computerized physician order entry (CPOE). He told his board of directors he would not oversee a rollout until he saw what he considered a successful implementation.

That meeting happened to coincide with the iPad's initial release. He embarked on the current project after testing four iPads when clinical and IT leaders convinced him it would work—and after he sunk resources into making it work better than the initial two-week tests that were run virtualized to the iPad.

"The physicians came back and said 'This is game-changing, absolutely game-changing,'" said Potter, adding that it was nonetheless "painful" to watch physicians struggle with the virtualized interface, even as they delighted in demonstrating how they were using the iPad to view medical images, charts and labs.

Ottawa Hospital—spanning four hospitals and 1,300 beds—has deep pockets for such a project, which went live on the first 1,000 iPads last January and will be tripling in size in the coming months. However, the productivity gains and inexpensive iPad hardware made it straightforward for Potter to convince the finance department that it was worth the capital outlay for in-house development and hardware purchase. That, and the fact that his development team can work faster and deploy apps tightly tailored to his hospitals' workflow.

So far, with the help of an ergonomics consultant who interviewed and followed physicians around to get an understanding of hospital

workflows, the software development staff has finished a dozen custom iPad apps that page and scroll in ways iPad users are accustomed to.

IPAD EHR MAY NOT COME TO THOSE WHO WAIT

For other hospital CIOs faced with iPad implementations, Potter agreed that tablet ownership is the first key decision to make. He felt it was easier to standardize development and security for a native iPad EHR implementation if the hospital bought them, and the IT staff wouldn't have to worry about developing apps for Android or BlackBerry operating systems. The facilities do allow employees to bring their personal iPads to work, but for iPad security purposes, they must agree to use software from MobileIron Inc. that gives IT staff control of an iOS device when needed.

None of the iPads, by the way, have been lost or stolen yet. Users "cherish" the devices more than they do others, Potter said, adding that he's seen physicians return home at the beginning of a shift to fetch an iPad left behind; the time lost driving back and forth is worth not struggling with another device.

After that, the next key decision is deciding how fast you want to move. This can depend on whether you trust your vendor on two counts—delivering an app, and delivering an app that will fit your hospital's way of working. Potter said that his EHR vendor probably wasn't going to be iPad-ready for 18 to 24 months after the device came out in early 2010.

That wasn't fast enough for Ottawa Hospital. "You have to go fast. I said to the board chair and the CEO, 'If you guys are serious, we've got to go fast,'" Potter said. One of Ottawa Hospital's goals is being recognized as a top-10 academic hospital in North America for patient safety and quality, and, Potter added, the board of directors saw the custom iPad implementation as a way to get there more quickly.

"Should a hospital be in the business of [mobile app development]? You could argue, probably no. But if we didn't want to stay in the middle of the pack and we wanted to move ahead in this mobility concept, we had no choice" but to develop without the EHR vendor, he said. ■

Don Fluckinger is features writer for SearchHealthIT.com. Write to him at dfluckinger@techtarget.com.

CHAPTER 3

SECURITY REQUIREMENTS FOR IPAD HOSPITAL USE

Whether hospitals roll out iPads with native applications on them or deploy a virtualized desktop for iPads, there are several key security measures that hospital IT leaders should take. **BY NARI KANNAN**

BOSTON'S Beth Israel Deaconess Medical Center is the teaching hospital of the Harvard Medical School, with more than 800 full-time staff physicians, nearly 1,200 full-time registered nurses and roughly 750,000 patient visits a year. Beth Israel has been using computer technology since the 1960s. Before the iPad came along, physicians and nurses used desktops and laptops to access a browser-based electronic health record system (WebOMR), computerized physician order entry system (CPOE) and a number of other applications. When it came to extending these systems to iPads, Beth Israel allocated Web access to these applications with virtual desktop extensions to iPads. Once users log in with a username and password, the iPad becomes their virtual desktop.

The Ottawa Hospital, meanwhile, took a different route. Instead of rolling out a virtualized environment to allow physicians to use personal iPads to access EHRs, Ottawa Hospital purchased thousands of iPads

ONCE USERS LOG IN WITH A USERNAME AND PASSWORD, THE IPAD BECOMES THEIR VIRTUAL DESKTOP.

for its clinicians and hired software developers to write native applications, in the process creating a secure portal between the hospital's EHR system and the iPads. This means that data may be downloaded on to the iPads and may have to be erased

when devices are switched off or leave the hospital campus.

Keeping these two different ways of rolling out iPads for use in hospitals in mind, a combination of the nine following security requirements are typically deployed.

- **Username, password login.** In iPad roll outs in hospitals with virtual desktop environments, you may already need a username and password to get the virtualized system started up. When hospitals are using native applications, they still need access to back-end servers. These need to selectively download data that is needed by an app and delete it when done. Native apps also need username and password logins to make them as secure as virtualized rollouts.

- **Role-based login.** Not all applications may need to be accessible to all users in a hospital. Role-based logins may be already set up on iPads being used in a virtualized environment. When using native apps, they may need to be designed and implemented within the apps themselves.

- **Copying, printing control.** Since it is possible to copy and even print data from medical records in iPads, some level of control is needed. Role-based logins can be used in iPads to enforce this security measure. Users are assigned roles as clinician, nurse or hospital administrator; their roles, in turn, can permit them to copy or print at the data level.

- **Encrypted data transmission.** Virtualized desktop environments may already have 128-bit, built-in encryption of any communication, including data to and from iPads. If native applications are developed for iPads, then those apps may need to implement this level of encryption when communicating with servers.

- **Isolated special subnets.** When using tethered computers such as laptops and desktops, administrators usually have better visibility, control, network speeds and service levels. Mobile devices such as iPads may need isolated special subnets, meant only for them. It may also be necessary to track where the devices access the network, for the sake of iPad security as well as performance—mobile devices are subject to differing signal strengths, and certain signals may not provide the bandwidth needed to use certain applications.

- **Remote wipe capability.** Virtualized desktop roll outs may or may not make use of local storage. Native apps may invariably use local storage, even if it's only for temporary download of medical data. In either

case, and as noted in Chapter 1, iPads may need to be remotely wiped when they are switched off or wander off from the main campuses where access is allowed. In addition, if iPads are lost, misplaced or stolen, the same remote wipe capability may be needed.

- **Remote autolock.** Both iPads and iPhones support remote autolock so that the devices themselves may be locked, if lost, misplaced or stolen. They also require long pass codes to reactivate when located again. All data can be erased automatically after 10 failed attempts at entering the pass code. Before iPads—whether they are owned by clinicians or supplied by the hospital—are rolled out, they may all need to be registered with the hospital and this feature enabled.

- **Authentication mechanisms.** Additional authentication mechanisms may need to be implemented, using technology such as real-machine identification and a hospital-assigned, machine-specific ID that is given to a clinician. With both types of IDs, the iPad will be allowed to access the network. This is an additional security precaution to make sure that an iPad is really the iPad it says it is and, on top of that, to ensure that the user is also authenticated.

- **Additional anti-virus protection.** Even though anti-virus protection is not available on iPads per se, additional standardized anti-virus/malware protections may be needed on the server side when iPads are rolled out. This may be true for both virtualized or a native app roll out.

Doctors and nurses have started bringing their own Apple iPads into the hospital—and demanding access to hospital applications on them. However, iPads pose many security problems. Hospital IT departments are responding in two main ways—virtual desktop deployment or customized native iPad applications. Many hospital systems are also finding that security precautions can be enumerated and implemented in a systematic way. The additional time, effort and resources spent on these security requirements seem to be a small price compared to the benefits that clinicians seem to be reaping from the use of iPads in hospitals. ■

Nari Kannan is the Chief Executive Officer of appsparq Inc., a Louisville, Ky.-based mobile applications consulting company. He has more than 20 years of experience in information technology.

CHAPTER 4

EFFECTIVE IPAD SECURITY POLICY ENFORCEMENT

The use of iPad management tools, including third-party tools as well as those that come with the device itself, will help health care organizations enforce the security, privacy and risk management policies needed to let physicians use the devices. **BY LISA PHIFER**

AS IPAD POPULARITY grows among health care professionals, IT and network administrators must find more effective ways to manage associated security risk. Policies to ensure the safety of electronic medical records and communications are essential, but don't stop there. Use iPad management tools to deliver reliable, scalable policy enforcement.

Before tapping the iPad to enhance the quality and efficiency of medical service delivery, administrators must identify related threats and apply compensating controls to manage risk.

Fortunately, Apple Inc.'s iOS 5—the operating system that powers the iPad—supports many mobile security best practices, including authenticated access control, full-device encryption, and automated or remotely-initiated data wipe. For secure communication, iOS 5 supports Secure Socket Layer/Transport Layer Security (SSL/TLS),Virtual Private Network (VPN) and Wi-Fi Protected Access (WPA2).

However, iPads must still be provisioned for safe use. As pointed out in previous chapters, settings must be changed to require a password and auto-wipe after repeated failures, and permission must be granted to remotely find or wipe a lost or stolen iPad. Exchange, point of presence (POP), or Internet Message Access Protocol (IMAP) credentials must be entered before email messages, contacts, and appointments can be synchronized. Private wireless local area network (WLAN) and VPN connec-

tions cannot be established until network settings have been configured.

Health care organizations cannot rely upon end users to configure these controls. Regulations require such organizations to ensure and document proper provisioning, promptly detect and remediate noncompliance, prevent unauthorized access to sensitive systems and report potential electronic medical record breaches. These needs can be met by leveraging the iPad's native management interfaces.

ADMINISTRATORS CAN PROVISION ANY IPAD BY INSTALLING CONFIGURATION PROFILES: XML FILES CONTAINING DESIRED DEVICE SETTINGS.

IPAD CONFIGURATION POLICIES

Administrators can provision any iPad by installing Configuration Profiles: XML files containing desired device settings. For example:

- A Passcode Policy profile can require a passcode while setting minimum length/complexity and maximum age/retry rules.
- An Exchange profile can configure an email account with a specified server name/address, email address, username, and password/certificate while preventing message forwarding or requiring Secure Multi-Purpose Internet Mail Extensions (S/MIME) signing and encryption.
- A VPN profile can provision an iPad with a Layer Two Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP) or IPsec tunnel endpoint, including shared secret or certificate and XAUTH username.
- A Wi-Fi profile can configure a wireless LAN's network name, encryption type and pre-shared key or Extensible Authentication Protocol (EAP) credentials, including username, identity, and password or certificate (see **FIGURE 1**, page 15).
- A Restrictions profile can disable built-in iPad capabilities, including camera, screenshot and user acceptance of untrusted web server certificates.

These and other iOS Configuration Profiles can be locked to prevent snooping and removal. For example, an encrypted password-protected VPN profile could be emailed to every employee given access a pri-

vate network, but only users who knew the profile's password could successfully install it. However, authorized workers could still install the same profile on unapproved devices—such as personal iPhones—or change VPN settings. Fortunately, device enrollment and on-going monitoring can prevent those pitfalls.

IPAD DEVICE MANAGEMENT

In fact, Configuration Profiles can be installed in four ways: pushed from the iTunes Configuration Utility to a USB-connected iPad, emailed to an iPad user, downloaded onto an iPad from a website, or installed by a mobile device manager (MDM). The latter requires an iPad user visit the organization's MDM enrollment portal.

During enrollment, the user is authenticated and the iPad itself can be checked against policy. Only authorized iPads can complete MDM enrollment, during which they are issued a device certificate and must grant permission for MDM to management and monitoring (see **FIGURE 2**, page 16). Thereafter, the organization's MDM can install, replace,

Figure 1: ***Setting Wi-Fi Profile in iPhone Configuration Utility***

and remove Configuration Profiles and, perhaps, Application Profiles as well.

To exert this centralized IT control over iPads, a health care organization must either install its own iOS-capable MDM platform or purchase a managed or cloud MDM service. MDMs that can manage iPads are readily available from dozens of vendors, including AirWatch LLC, Boxtone Inc., Fiberlink Inc., McAfee Inc., Mobile Active Defense Partners LLC, MobileIron Inc., Odyssey Software Inc., SOTI Inc., Sybase Inc., Symantec Corp., Tangoe Inc., Ubitexx (now owned by Research in Motion Ltd.) and Zenprise Inc. While each MDM is to some degree unique, all use Apple's Push Notification Service (APNS) and native iOS MDM APIs to communicate securely with enrolled iPads.

These APIs support iPad device enrollment, device provisioning —based on Configuration Profiles —device monitoring, application install/license/remove—based on Application profiles—and IT-initiated remote lock, passcode clear, and wipe actions. MDMs leverage these APIs to deliver near-real-time visibility and control over enrolled iPads, including security policy enforcement. In addition, some vendors offer an optional iPad MDM application that users can download from Apple's App Store and install to deliver deeper device insight—most notably, jailbreak detection.

Figure 2: ***MDM Permission Management and Monitoring***

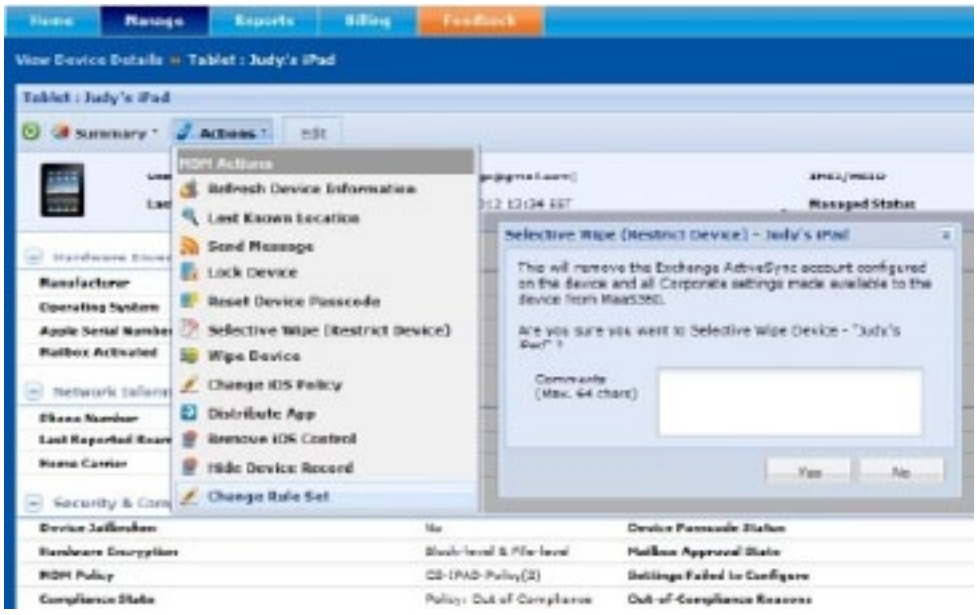
HOW MDM CAN ENFORCE IPAD SECURITY POLICIES

MDMs not only make iPad management more scalable; they can help any organization report on security posture, detect policy violations, and take immediate action to prevent network intrusion or data breach. Such management tools are especially important in regulated environments such as health care.

For example, MDM enrollment can stop a physician from manually provisioning her own personal iPad with an otherwise valid Configuration Profile. Instead, each physician can be invited to visit the hospital's MDM portal and enroll his or her own iPad, linking each authorized device to user credentials and associated security policies. At any time, IT administrators can now generate reports listing all authorized iPads, who owns them, when they were provisioned and the last time they were contacted.

Suppose that policy requires passcode authentication, full-device encryption, and secure WLAN access to reach the hospital's Exchange server. If a physician should misplace his or her iPad, IT can immediately lock the device and disable both WLAN and Exchange access by removing those Configuration Profiles (See **FIGURE 3**). Should the iPad go missing indefinitely, IT can

Figure 3: ***Setting Configuration Profiles to Enable Remote Wipes***



remotely wipe the entire device or simply remove MDM control—a step which also removes all settings, applications, and data installed by the MDM. Here again, MDM reports document when lock or wipe actions were taken.

Over time, unmanaged mobile devices have a bad habit of drifting into non-compliance. For example, users may install risky applications, visit malicious websites, or connect to unencrypted WLANs, thereby endangering sensitive data and credentials stored on the device or enabling network intrusion. However, an iPad continuously monitored by MDM can routinely report its security posture—for example, helping IT spot any iPads running black-listed applications or connecting to open WLANs. Depending on the violation and configured security policy, MDM may notify the administrator or quarantine or wipe the offending device.

Ultimately, MDM cannot deliver total control or support every possible security policy. For example, Apple APIs do not allow MDMs to remove blacklisted applications. However, these management tools can help health care organizations reap the benefits of iPads while effectively and reliably managing associated risks. ■

Lisa Phifer is president of network security consultancy Core Competence Inc.

TechTarget

Managing iPads in the Hospital is a SearchHealthIT.com e-publication.

Brian Eastwood
Site Editor

Linda Koury
Director of Online Design

Nari Kannan
Lisa Phifer
Contributing Writers

Jean DerGurahian
Editorial Director

Anne Steciw
Associate Site Editor

Craig Byer
Assistant Site Editor

Don Fluckinger
Features Writer

Stephanie Corby
Associate Publisher
scorby@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com