WHITE PAPER:
MOBILE ENTERPRISE MANAGEMENT

Mobile Enterprise Management: Improving Healthcare While Protecting Patient Information

Who should read this paper

Healthcare CIOs and IT security and compliance officers who must manage devices, applications, and data outside the firewall or in the cloud, while enabling a seamless user experience and protecting and securing patient information.

Confidence in a connected world. Symantec.

Content

Mobile Enterprise Management: Improving Healthcare While Protecting Patient Information

Mobility and BYOD (bring your own device) represent significant trends in healthcare information access today. According to a recent survey, 93 percent of physicians are now using mobile health technology daily.[1] And it's no surprise. Physicians, by nature of their jobs, are mobile. Visiting patients at the bedside, traveling from their offices to clinics or seminars, and making rounds at affiliated hospitals, physicians are always on the go. The arrival of mobile technology has been a boon for these doctors, who can now, regardless of physical location, use mobile devices to:

- Communicate and collaborate with colleagues, team members, and patients
- Review test results
- Electronically prescribe medications
- Generate clinical documentation
- View X-rays and other images
- Capture patient billing details
- Review online healthcare resources for medical reference materials

This kind of flexibility allows doctors and other medical workers to ultimately provide better care to their patients. Streamlined workflows and the immediate availability of patient data for quick decision-making improve productivity and efficiency, which has a positive impact on clinical outcomes as well as business parameters.

The challenge: protecting patient data in the age of mobility

Along with its many advantages, mobility presents a serious set of challenges for compliance officers and healthcare IT departments. Because mobile devices are inherently less secure, more vulnerable, and more complicated to support and maintain due to a wide range of device options, operating systems, and applications, healthcare organizations were initially reluctant to support physicians' personal mobile devices on hospital networks.

Beyond those challenges lies the real issue: the specter of security breaches via loss or theft of the device, attacks on the device in an attempt to steal information or otherwise compromise the device, and risks to the larger network resulting from a device's gateway access to that network. Unfortunately, it's not terribly difficult for a moderately talented hacker to break into a mobile device and wreak havoc. Security breach problems have always existed, and today's mobile devices—especially those that are unmanaged or unknown—make the threat even more daunting.

In the highly regulated healthcare industry, HIPAA security and privacy rules, as defined by the Department of Health and Human Services, require healthcare organizations to protect patients' health information. Failure to do so results in stiff penalties and reputation damage. According to the HITECH Act 2009, in the event of a breach, healthcare organizations can be fined upwards of $1.5 million per incident and are required to notify the local media if the breach involves more than 500 patient records.[2]

If a physician-owned mobile device introduces malware to a hospital's network, it can lead to performance degradation and potential security breaches. Fortunately, increasingly sophisticated solutions are appearing on the market to help healthcare IT minimize exposure and manage the issues.

[1] http://www.himssanalytics.org/about/NewsDetail.aspx?nid=81558
[2] U.S. Department of Health and Human Services, HITECH Act Enforcement Interim Final Rule, 2009

From the BYOD trend to wireless networking that supports radio frequency identification (RFID) technology, the following examples highlight how wireless and mobile devices are improving healthcare, while also protecting health information:

Instant access to patient data

A community-based physician on hospital rounds uses his iPad® to access patient information while connected to the hospital's network. Another doctor uses her smartphone to collect data at the bedside and access medical records and clinical data, enabling her to make faster and more salient decisions.

Biomedical devices

Wireless medical devices record and manage patient information. X-ray, magnetic resonance imaging, bedside monitors, and CT scanning systems capture and transfer medical data over the network and route that data to central data storage. Primary care doctors are monitoring their elderly and hospice patients via remote patient health monitoring made possible by mobile devices.

Pharmacy management

Pharmacy benefit managers use mobile apps to connect patients to appropriate online care information; encourage healthy behaviors, such as improved diet, exercise, and smoking cessation plans; deliver compliance alerts; suggest prescription drug purchasing channels; or generate medication reminders.

Internet access for patients and hospital visitors

People have become accustomed to connectivity. By providing Internet access, hospitals can help patients and their relatives stay in touch with loved ones back home and elsewhere.

Tasks on the go

A primary care physician uses her mobile device to conduct a variety of daily transactions, such as referring a patient to another doctor, sending an electronic prescription, checking a lab result, or ordering an imaging test, each of which interacts with a certified electronic health record (EHR).

Discharging patients

A discharge nurse uses a tablet to set up a video-conference among all involved parties regarding a patient's condition, follow-up care, and warning signs. They are shown images, test results, and medication procedures, and given instructions on follow-up care, pharmacy needs, medical appointments, and ongoing treatment—all of which can reduce confusion, misunderstandings, and re-admission.

Reviewing medical images

A physician uses a smartphone to review an X-ray or other image and is able to instantly collaborate with colleagues to discuss the case at hand and agree on the best course of action.

Improving collaboration

A patient is scheduled for hip replacement surgery but his EKG is not stable. The orthopedic surgeon requests a video consult with a cardiologist. Together, they view the patient's EKG, surgical X-rays, and medication list. They invite the pharmacologist to the meeting, who determines that the medication is the problem. A new medication protocol is ordered, and surgery is postponed until the patient stabilizes.

The solution: mobile enterprise management

These examples, while clearly beneficial, also strike fear into the hearts of healthcare CIOs struggling to comply with complex rules designed to protect and secure patient information. The challenge is to enable a seamless user experience, while also managing devices, apps, and data that reside outside the firewall or in the cloud, without compromising security or privacy.

The first step is to think about security strategy. Identify who can use personal mobile devices on the hospital's network, which devices, operating systems, and application software will be permitted, and how mobile devices will be managed, secured, monitored, and supported.

After that, take a look at the next-generation network management solutions emerging on the market. The best of these solutions support secure deployment, management, and monitoring for a wide range of Wi-Fi–enabled devices across the organization. Specific security controls include data loss prevention, encryption, mobile device management, and mobile application management tools, as well as strong authentication to endpoints and devices.

Mobile device management (MDM) software was the first solution to appear with the arrival of smartphones and tablets. MDM simplifies the management of clients and servers and reduces IT costs. For example, a strong MDM solution can remotely reset a device, conduct over-the-air hardware, software, and network inventories, deliver software or automatically repair apps, create reports, and integrate with security solutions—including file encryption and device lock and wipe capabilities—representing a significant help to administrators. However, as people began leveraging apps to access, store, and transmit more and more corporate data, MDM was no longer sufficient on its own.

Mobile enterprise management: a convergence of solutions

Today, there is a growing convergence between MDM and mobile application management (MAM). In fact, IDC has defined a new category, called mobile enterprise management (MEM), that combines the two technologies.[3]

While MDM manages mobile phones, tablets, embedded systems, and printers, MAM attends to the management of applications and data. A mobile hypervisor acts as a dual personality, allowing users to switch between personal and work "personas."

The new MEM solutions provide more granular control over applications and data than the traditional MDM solutions. Leading solutions can perform MDM actions like lock, wipe, ping, and dissociate device. And they go further by allowing administrators to access key corporate assets, such as email, calendars, and even secure profiles for enterprise Wi-Fi and virtual private networks (VPNs). They ensure regulatory compliance by enabling advanced security settings on the various devices. And they can limit device functionality and set or reset password complexity rules. In short, they enforce enterprise IT policies across a heterogeneous infrastructure of devices.

When looking for a solution, make sure it addresses:

- **Device-layer security:** The best solutions integrate application and device security and provide complete control over the hardware. This means knowing where the device is at all times, yet allowing the user to work productively. Device-layer security means that tracking, full wipes of the device, and automated process can all be controlled by the healthcare organization. Furthermore, IT can ensure that the device is compliant with a wide array of regulations before a user is allowed to access sensitive data from that device.
- **Application-layer security:** MAM segments the physical device from the applications that are being delivered. These platforms allow healthcare administrators to create application-independent wrappers or application-specific micro-VPNs, so the mobile devices don't need a VPN client to connect into a corporate network. Rather, the device can authenticate and gain access to internal resources based on

[3] http://www.symantec.com/en/ca/content/en/us/enterprise/white_papers/b-mobile-enterprise-management-security-idc.pdf

the application that is needed. In this scenario, the user can still use a personal device instead of a corporate one. A client on the device separates the user's personal information from corporate data.

- **Information-layer security:** The constant need to secure data holds is imperative for the healthcare world. Now, as an added layer to the security model, information delivered to devices over the cloud can be secured and controlled. New types of file and data-sharing solutions take data security to a new level. Healthcare organizations can recreate environments within their own data center walls, gaining full control over the data—where it's being delivered, who's accessing it, and how it's being shared. Further, these technologies directly integrate with both MDM and MAM solutions. Now, healthcare organizations can regionally lock down the location where information is being accessed and synchronize it with dispersed users. In fact, data-layer security and integration technologies now allow administrators to replace "My Documents" and home directories with these data-access platforms. As a result, users have their information available to them within their familiar desktop settings.
- **User-level security:** Administrators can secure the end user by abstracting the settings and profile layer. This means settings, personalization elements, and other user-related data can be delivered to any device on any operating system. Administrators can place the user's settings into a container and allow it to carry over to various platforms. This means that working with different versions of software or even operating systems is no longer an issue. Instead of allowing services such as Microsoft® to manage profiles and user settings, the job is transferred to a database that is replicated and secured.

In addition to securing, monitoring, managing, and supporting mobile and other Wi-Fi devices connected to the hospital's network, leading mobile device and application management tools offer remote application distribution, a sandbox to remotely wipe patient data from mobile devices when necessary (or even automatically after a pre-ordained period of time), and the ability to remotely configure mobile devices to meet enterprise IT policy requirements.

In addition, a robust MEM tool includes authentication and single sign-on for both the portal and wrapped applications. Wrapped applications contain a management layer that doesn't require changes to the underlying application. Look for integrated single sign-on functionality for wrapped in-house apps, leveraging popular authentication methods including Active Directory®, LDAP, SAML, and SiteMinder®. The best products extend authentication and single sign-on to cloud and wrapped apps as well.

Finally, a good solution can enforce a secure connection—SSL or HTTPS—for apps and block apps from accessing unauthorized or malicious websites, by mandating an SSL connection and the presence of trusted certificates to ensure information security for data-in-transit. This prevents data loss and simplifies compliance by controlling app communication without requiring a costly VPN.

Conclusion

Mobility is here to stay, and that's a good thing. Both patients and doctors are benefitting from mobility as it helps to improve care delivery. However, with these exciting changes come risks. Patient data must be protected. The best course of action is to derive a mobility strategy that clarifies what's needed. Write policies around which devices employees can use, where they can store medical data, and how IT can enforce those rules. There are many approaches to mobile enablement—including MDM, MAM, or a combination of the two—that can help you protect data, while taking advantage of the windfall of efficiencies that come from mobility.

Achieve productivity and protection through an integrated approach

Symantec™ Mobile Management Suite is a comprehensive mobile protection solution that enables a seamless user experience across multiple mobile deployment models including enterprise-owned, employee-owned (BYOD), or a hybrid of both. The suite addresses the five essential pillars needed for a comprehensive mobility strategy: user and app access, app and data protection, device management, threat protection, and secure file sharing.

To learn more about enterprise mobility that offers complete protection without compromising the user experience,
visit http://go.symantec.com/mobility.