# Security of Mobile Computing Devices in the Healthcare Environment

**11/1/2011**

A White Paper by the HIMSS Mobile Security Work Group

# Table of Contents



 

## Introduction

In the past few years, the technology landscape has been drastically changed by the proliferation of consumer-focused mobile computing devices. These devices, primarily smart phones and mobile tablets, are a new type of platform – less power than laptops and workstations, but with more functionality and connectivity than traditional phones and personal digital assistants (PDAs). And their popularity has driven a significant demand for their use in business.

This increasing use of mobile computing devices is perhaps nowhere more noticeable than in the healthcare industry. Health services providers and medical vendors are finding new and innovative ways in which to use this new platform to better support patient care. And for the healthcare businesses, this represents potentially lower costs and higher quality of service.

Imagine a scenario where a physician walks into a patient's room with an electronic device about the size of a medical chart. She sits down right beside the patient and begins to review the latest laboratory results – showing the patient and his family graphically how the numbers compare with normal results and explaining what the deviations mean. She then moves on to reviewing the latest x-ray and MRI images, zooming in on areas of interest. Next she moves on to the historical telemetry information, noting a restful sleep with normal activity. She cancels the patient's daily medication orders and signs the discharge order as she is dictating her notes through medical transcription software. Later that night, the patient calls the Emergency Department reporting a strange feeling. The hospital gets in touch with the physician at her home. She uses her mobile device and advises the patient that it is likely just a reaction to a particular medication, and prescribes a mild sedative.

### Past, Present and Future of Mobile Computing Devices

In the past, mobile medical devices were clunky specialty machines or cumbersome multi-purpose machines. This included early attempts at bringing

**Example:** One solution was to mount a laptop on a tall cart that could be wheeled around, attached to a large battery. But the cart was top-heavy and hard to control. The batteries frequently failed to maintain their charge. Plugging the carts in meant taking up hallway or nursing station space. The carts themselves cost more than the laptops. This expense meant there were never enough to go around and so carts were frequently "borrowed" from one area to another, making tracking difficult. Worse, these carts were sometimes stolen and not replaced due to the expense.

computer workstations to nursing stations, mounting them on carts, or installing them in hallways or patient rooms. Those solutions frequently failed in real-world healthcare environments, largely due to inconvenience. The solutions were either too bulky, inconvenient to use, had a steep learning curve, too expensive to widely deploy, etc.

The failure of these solutions was a costly and frustrating situation for patients and providers alike. The security model in this case was the traditional security model used for workstations and laptop computers, as well as for specialty mobile devices.

Today there are as many different deployment models for mobile computing devices as there are organizations. Few standards exist for mobile computing devices, either within the healthcare industry or the broader IT industry. But one thing is certain – employees are not waiting for guidance to be provided. Instead, they are starting to use mobile computing devices for work, whether or not their employers know or approve of the use. Security guidance is also lacking.

The management of mobile computing devices can be categorized into one of several models:

- **Ad-Hoc.** When a patient care provider wants to use a mobile computing device, they use their own, and IT has little to no knowledge of it. No official policy exists within the organization to govern use of the devices.
- **Uncontrolled.** There is an informal policy or a formal policy that is not enforced and often overridden by management. A mixture of ownership and management models exists between employees and the organization. Device and application support is provided by some combination of employee, company, wireless carrier and device manufacturer.
- **Controlled.** There is a formal policy that is enforced. Device ownership is clearly defined, though it may be mixed between company and employees. At a minimum, management of business applications is centralized within the company.
- **Owned.** A formal policy exists and is followed. The organization owns and manages all devices, including subscriptions and maintenance. All applications are maintained centrally by the organization.

 

In the future, the goal is for mobile computing devices to be fully integrated into the healthcare environment. Guidance would be provided both by the broader IT and security industries and by the healthcare industry. And each company would have a well-defined policy on mobile computing device use.

## Focus and Goal of this Paper

The focus and goal of this paper is to provide an information resource about mobile computing device security to healthcare information technology leaders. This is not meant to be a blueprint for how an organization should deploy mobile computing devices; instead it provides the necessary groundwork for the organization to take the steps to formally define policies, procedures and processes.

The HIMSS Mobile Security Work Group feels that it is important to provide this guidance now. The use of mobile computing devices in healthcare organizations is growing very quickly, whether endorsed by management or not. This use is likely to continue to grow and it must be accommodated somehow. Mobile computing devices pose some of the biggest risks to security and compliance today. And these devices are being rolled out at a rate that is outstripping our ability to adequately secure them. Research suggests that the market for mobile computing devices in the healthcare market is set to go from $100M today to $1.7B in 2014.[1]

This paper will focus on mobile computing devices such as smart phones and tablets. These are devices which offer more computing power than a traditional PDA or phone, but less than a laptop, and are built on a specially designed mobile platform or operating system. Devices such as laptops, portable storage devices, and cameras, although used often in a healthcare setting, will not be reviewed. Although mobile computing device management and policies will be touched on, this paper is intended to discuss the security and compliance ramifications only. In the near term, the Mobile Security

**Why not laptops?** Laptops follow a more traditional security model, based on well-known operating systems. Because there are many articles available on how to secure these devices, we will focus on smart phones and tablets.

[1] http://searchhealthit.techtarget.com/news/2240025600/Mobile-health-market-on-verge-of-explosive-growth-report-says

 

Work Group will be developing a "Mobile Security Toolkit," which will contain other various items, such as example policies.

## Importance of Mobile Computing Devices in Healthcare

In healthcare environments, it is important to understand the benefits of effectively using mobile computing devices. Mobile computing devices allow for quicker and simpler access to data, resulting in better care for the patients. When a clinician can get access to lab results while quickly viewing results on his mobile computing device, and then based on those results react and advise other providers, the effect of mobility on patient care is easily seen. With clinicians becoming less dependent on desktops and laptops, they will be more able to provide care in any environment.

Healthcare facilities today support hundreds, and in some cases thousands, of desktop computers. Most of these are large, stationary form factor devices. Often clinicians are required to use multiple desktop devices each day. Each time they access data from a new device, they must be authenticated to ensure compliance with regulatory requirements. With mobile computing devices assigned to each user, the total number of devices required to accomplish patient care decreases. While the use of mobile computing devices may not be the replacement for all aspects of our healthcare applications and systems today, many applications and uses can be accommodated on these devices.

Therefore, the benefits of enabling a secure mobile computing device platform are clear. In the scenario described in the introduction section above, several benefits for patient care exist. The mobile computing device has become the interface to many different types of equipment, such as radiology stations, paper charting, nursing desktop computers, biotelemetry monitors, dictation stations, and prescription pads. Mobile computing devices create more free space, less clutter and lower costs, while delivering more services more efficiently, with a lower error rate, and through linking with electronic health systems.

The following is a summary of some of the benefits of mobile computing devices in healthcare:

 

**Patient Care**

- *Increased efficiency of the healthcare provider when with the patient*: The care provider does not have to go from machine to machine, room to room, back and forth to a computer terminal, etc.
- *Real-time visibility into the patient's condition*: Instead of waiting for lab results to be sent, x-ray images to develop, charts to be read, telemetry to be processed, healthcare professionals have this information at their fingertips.
- *Increased patient participation in their own healthcare*: This lightweight and interactive technology should allow the caregivers to be physically closer and more interactive with the patients. This provides a sense of ownership, meaning that the patients and their families are more likely to absorb and interact with the information. The interaction can give more information to the physician who can then make a better diagnosis. The ownership leads to higher rates of acceptance of the diagnosis and the following of orders post-diagnosis.
- *Integration with electronic medical records*. The use of electronic medical systems is intended to reduce costs and error rates. Mobile computing devices drive further adoption of these systems.[2]

**Cost**

- *Reduced capital cost*: Specialty devices are expensive and often have limited functionality. As a result, it is very expensive for hospitals to support many of these devices. With mobile computing devices, healthcare organizations can reduce the number of devices needed and thus bring down costs.
- *Reduced maintenance cost*: Things break. Some things break more often than others. There's nothing more frustrating or costly than a device that is not operational when it is needed most. Fixing these specialty devices tends to be more costly than fixing or replacing a small mobile computing device. Support and maintenance contracts often equal the cost of the device over three to four years.

[2] http://www.eecs.harvard.edu/cs199r/readings/RAND_benefits.pdf

 

- *Reduced training cost*: With a single device, training costs go down compared to the costs to support many devices. And if that single device is one that the healthcare provider also uses for personal use, this familiarity will reduce the cost of training even further.

**Other**

- *More free space*: Space is at a premium in hospitals. Large form factor machines take up much needed space in areas such as nursing stations, patient rooms, hallways, and patient care rooms that have been converted to storage areas for specialty equipment. Mobile computing devices allow much of this space to be reclaimed (see the example box on page 3).
- *Hire and retain healthcare providers*: Physicians and nurses want the latest technology. Healthcare organizations that ignore this are bound to lose employees to those that provide and/or support mobile computing devices.
- *Improving emergency room processes*: By freeing up admission nurses from sitting behind their desks, mobile computing devices can improve the process of admitting patients. A patient with a trauma no longer has to limp over to the desk and sit uncomfortably while doing the paperwork. And it is easier for non-ambulatory patients to be admitted if the electronic paperwork can be delivered to them.

As healthcare organizations today are permitting the use of mobile computing devices, the next logical step requires a plan to provide an effective method to ensure the security of data being accessed using these devices. This involves implementing strong access controls both at the device and network levels, as well as ensuring identification and authentication, audit, and other necessary controls. In an ideal environment, as mentioned above, we permit only applications which allow the viewing of our data locally on the mobile computing device but do not permit the storage of sensitive data on the local device without strong encryption. This ensures that the user is viewing only the latest data available and should the device be stolen or lost, no unauthorized use of data can occur. However, if data is stored on the local device, appropriate levels of data encryption should be in place.

 

## Areas of Concern with Mobile Computing Devices in Healthcare

### Addressing Risks

From a healthcare perspective, several important risks exist regarding the security of mobile computing devices, including the ubiquitous proliferation of the devices, the complexity involved in securely managing the devices, the costs necessary to provide adequate security, the potential for loss or theft of the devices, the growing threat of malware, and the limitations involved in using the small form factor mobile computing devices.

Today, virtually everyone has a tablet, smart phone, or other mobile computing device, either for work or personal use. The healthcare organization must also consider whether it will permit the use of both organizationally and non-organizationally owned devices on our networks. If it only permits organizational-owned devices, it must determine how to control/prevent the access of the non-organizational devices to their networks. If the organization permits the use of personal devices, does the organization provide a stipend to the employee to purchase the device and associated service (cell or broadband)? If it permits employees to use their personal devices, how does the organization ensure that only authenticated users (and devices) are being used for business purposes?

Another important question that must be addressed is how does the organization ensure that its users of personal devices implement effective security controls on their devices, including access controls, malware protection, etc.?

Healthcare organizations must next decide what access should be given to patients and visitors. It is important to remember that it's not only staff members who use these devices, but also patients, families, and their friends. As the number of mobile computing devices has grown, the number of patients who want to keep up with their email and social networks has also grown. Hospitals and points of care need to consider providing secure access for these patients, ideally via a "guest" network that is separate from the internal hospital network.

## Issues and Considerations

In today's healthcare environment, budgets are a major issue for every organization, and each department and employee wants equipment to help them do their job better. Finding the right mix of what is an actual requirement and what is a "nice to have" is an issue for every organization. Determining which roles in the organization are best served by the use of mobile computing devices, and then determining how much the organization can afford to spend on the devices are only the first steps in the process. Determining which devices provide the organization the best assurances that patient data will be handled according to all compliance requirements is critical, but even more important than that is that patient data will not be at increased risk based on the introduction of mobile computing devices into the environment.

Millions of mobile computing devices are reported stolen each year[3] around the world.[4] Asurion[5], a leading electronics insurance agency, reports that over 56% of users report losing or misplacing their phones for short periods of time each month. And over half of all devices are reported to contain some company information.[6] Most breaches reported to the Department of Health and Human Services so far under HITECH have been theft or loss of mobile computing devices resulting in the exposure of millions of patients' protected health information (PHI).[7] So, based on these facts, how long does it take someone who has the knowledge to remove (or copy) all the data from a device? If an organization permits the use of mobile computing devices on its networks, it must take precautions to make sure that this data is not compromised if the device is lost – either through encrypting the sensitive data as it is stored (even briefly) or by disallowing storage altogether.

When devices and their operating systems are initially released, the likelihood of malware (virus, Trojan, etc.) is limited. As the popularity of mobile computing devices increases, so too does the possibility that someone will create malware that is intended to impact its use or compromise

[3] http://www.imhonest.com/InterestingFacts.jsp
[4] http://www.guardian.co.uk/money/2006/may/16/internetphonesbroadband.phones
[5] http://www.asurion.com
[6] http://www.darkreading.com/cloud-security/167901092/security/news/229625511/half-of-lost-or-stolen-mobile-devices-store-sensitive-company-data.html
[7] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

 

patient data. In addition, the mobility of the device is as much an issue as an asset. Being able to use the device virtually anywhere in (or even outside) the facility is a positive. Areas such as basements, labs, radiology areas, etc., due to their construction and other factors, often restrict the ability to connect to network resources. However, recent strides in providing converged, broadband in-building wireless coverage, such as with distributed antenna solution technology, have greatly improved access to medical applications and devices.

The next consideration is the application developer; which devices or operating systems do they support (or support first)? Do they develop applications for a specific device because it is already in heavy use in healthcare, or do they create applications that are easily adapted to an assortment of devices? Remember, it has taken over 25 years of desktop computing to make effective use of them in our healthcare environments, and while many organizations have long since used desktops, only recently has there been an explosion of data sharing between health organizations.

In summary, there are concerns about transitioning to an environment where mobile computing devices are ubiquitous. The hidden danger in using mobile computing devices lies in their very power and portability. Security and privacy risks abound with mobile computing devices, as with any new technology. It is important for healthcare organizations to understand and mitigate these risks.

As seen in the table below, important areas of concern for mobile computing devices and applications are outlined. The Current Threat Level represents the current threats from a risk level ranging from low to high. A high value means these risks are persistent or frequent. A moderate value means the risk is present, but not frequent. A low value means the risk is theoretical or very infrequent (source material from OWASP[8], ENISA[9], ISACA[10] and collaboration with multiple security professionals).

[8] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks
[9] http://www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks
[10] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx

 

| Areas of Concern | Description | Current Threat Level | Privacy/ Security |
|---|---|---|---|
| **Device** | | | |
| Access Control | Controls in place over authorizing the user of the device. | High | P S |
| Encryption | Technology in place to protect data at rest. | High | P S |
| Updates | How and when the device is updated. | Moderate | S |
| Software Vulnerabilities | Weaknesses in the platform and OS which would allow for malicious attackers to access the device. | Moderate | S |
| Backups | How, when and where backups are handled. | High | P S |
| Mobile Malware | Viruses and other malicious software which can steal data, capture keystrokes or perform other negative actions. | Moderate | P S |
| Remote Management | How the device is managed remotely, if at all. This includes the ability to restrict application access, web access, encrypt data, remotely wipe, etc. | High | P S |
| Device-Specific Issues | Issues specific to mobile computing devices, but not other computing platforms. For example, the inability to truly erase mobile device storage. | High | P S |
| Platform-Specific Issues | Issues specific to each mobile computing device platform. For example, password storage, application back grounding or suspending. | Moderate | P S |
| **Application** | | | |
| Access Control | Controls in place over authorizing the user of the application. Includes session initiation and management, as well as least privilege access. | High | P S |
| Inappropriate Storage | What information the application stores and whether the level and sensitivity of information support local storage. | High | P S |
| Insecure Storage | For that data which should and must be stored, ensuring it is stored in an adequately encrypted or hashed fashion. | High | P S |
| Insecure Transport | Ensuring that sensitive data transported over the network is encrypted. This data includes usernames and passwords, but also session management information and other data. Does the application force the use of encrypted technologies? | High | P S |
| Updates | How and when the application is updated. | Moderate | S |
| Software Vulnerabilities | Weaknesses in the application which would allow for malicious attackers to access the device. | Moderate | P S |
| Backups | How and where backups are handled. | High | P S |

| | | | |
|---|---|---|---|
| Data Leakage | Does the application leak any potentially sensitive information, such as user name, device ID, location? | Low | P |
| Platform-Specific Issues | Does the application appropriately use, disable or work around platform-specific security issues? | Moderate | P S |
| Back-End Server | Is the server adequately secured? Is it protected from the normal application security flaws like SQL injection, misconfigurations, etc? Is it behind a firewall? | High | P S |

## Solutions and Tools

### The Challenge

The challenge involved in building a case for which solution or tool to implement can be seen by the rapidly changing mobile computing device market. Vendors in this space have been in this market for vastly different periods of time. Some are new to the management of mobile computing devices while others have many years of experience. Many vendors have a background in cellular, wireless, or personal computers, and are evolving their existing solutions to the newer mobile computing devices. As a result, feature sets vary widely. It is recommended that healthcare organizations develop a list of specific requirements, pick a solution that meets most of those requirements today, partner with a vendor that has a solid customer base, adequate funding to stay afloat in this quickly changing landscape, and a vision and willingness to partner and grow with its customers as requirements change.

Companies such as Gartner and Aberdeen have market analysts who closely watch this technology and monitor the vendors and their products. It is a good idea to take advantage of their research if possible. Another option is to ask mobile computing device vendors for reference calls of other healthcare organizations that have implemented their products or services. Success stories and challenges of healthcare organizations that have traveled the road you are about to embark on can be very valuable. Networking with your peers in healthcare is an excellent way to stay in tune with what others are doing, and to take advantage of the experience and knowledge they can offer (see www.himss.org for information on the newly formed HIMSS Mobile Security Work Group).

There are many questions to consider in the early evaluation phase. Hopefully the questions listed below will help healthcare organizations build a solid set of requirements that will help

 

them make the best vendor decision. Involve business stakeholders in this early decision-making. That investment will pay off dividends as the organization begins to test functionality.

## Early Evaluation Questions Healthcare Organizations Need to Ask Themselves

Questions to ask prior to a mobile computing device implementation:

1) Does your organization currently have a policy for use of smart phones in your environment (set expectations)?
2) Will you allow synchronization of email/data over the air or via workstations?
3) Will you allow smart phones to connect to your internal Wi-Fi network? Guest Wi-Fi?
4) Are you looking for asset control – information regarding the number of smart phones connected to your network – and the types of devices connected?
5) Will you require password controls with minimum length and complexity?
6) Do you want to lock/remote wipe devices after "n" number of login attempts?
7) Will you require inactivity timeouts?
8) Is device encryption required in your environment for data in transit or at rest? What level of encryption is supported, and how are the keys managed?
9) For lost or stolen devices, or when someone leaves the organization, will you be remote wiping the device?
10) Are you considering developing or enforcing an "Enterprise Applications Store?"
11) Do you need to routinely enforce compliance for connected devices with your policy – and disconnect non-compliant devices?
12) Can your existing NAC (Network Access Control) mechanism extend to mobile computing devices?
13) What liability considerations do you have? Will you support personally-owned devices, as well as corporate-owned? Will exceptions be allowed? If so, what is the documentation process necessary? You must demonstrate that you have clearly set expectations with users who may not be expecting a remote wipe of a personally-owned device. Employee signoff is highly recommended.

## Early Evaluation Questions for Vendors

Questions to ask your vendor representatives during early evaluation:

 

1) Review the vendor's record and obtain references who can share experiences. Focus on healthcare references.
2) How flexible is the management interface? Does the solution allow for multiple profiles or groups? Can you develop different sets of rules for each group?
3) Will your basic requirements/controls be met right away? Include administrative controls as well as security requirements. Examples might include the following:
    - Will you allow or disallow synchronization over the air (OTA) or via PC?
    - Will you allow or disallow roaming?
    - Will connectivity via Wi-Fi, Bluetooth, Infrared, and USB be allowed?
    - Will you require certification to identify the device to control access to email, Wi-Fi, etc.?
    - What are your password requirements?
    - Will you want to lock the device after a fixed number of login attempts?
    - Will you want an inactivity timeout to be applied to the device?
    - What are your data encryption requirements?
    - Will you require a remote wipe of the device if it is stolen or lost?
    - Will you allow personally-owned devices to connect?
4) Will the Mobile Device Management (MDM) software integrate with your local directory service (AD, LDAP)?
5) Are you planning to develop/support an "Enterprise Applications Store?" Do you require the ability to "white list" or "blacklist" certain applications?
6) What type of data do you expect will transmit through or be stored on the devices? How sensitive is it, and what is the worst case scenario in your environment if a device is lost or stolen?
7) Do you want the software to "push" apps and updates OTA?
8) Does the solution scale to your needs?
9) Where will the MDM server be located (internal network, DMZ, remote)? Are firewall rule changes required inbound?
10) Does the solution manage the operating systems you plan to support?
11) Does the solution support the email services you utilize in your environment?

 

12) Does the software allow for selective remote wipe of the device, leaving personal data in tact? This is especially important if you plan to support the connection of personally-owned devices to your network.
13) Can the solution detect and prevent or block "jailbroken" (IOS) or "rooted" (Android) devices from connecting to your network?
14) What backup solution is provided, and does it give you the protection you need?
15) Can I integrate policies into my existing BES environment?
16) Have the legal questions been answered?
    - What sort of agreement do the users have to sign if they own their device?
    - What expectations are you required to set with each user, whether the device is personally owned or not?
    - Note that in some jurisdictions, it is illegal to wipe employee data, even on a corporate-owned device.
    - Will the vendor offer assistance in developing these guidelines?

It is also very important to choose a vendor that will allow your organization to extensively evaluate their solutions. This will confirm that you are on the right track, and that the MDM solution you are considering is the right one for you organization's user base. Your vendor should be ready to partner with your organization and provide the level of professional services and ongoing support that it needs and that its users will expect.

## Case Study – Adventist Health System (AHS)

### Introduction

Like many other companies, AHS has been supporting standard email messaging on mobile computing devices for many years. Maintaining information security and compliance was relatively easy thanks to tools from Research in Motion (RIM), which allowed centralized management of the organization's Blackberry devices. This world began rapidly changing as other devices such as Apple's iPhone and Google's Android phones were introduced into the enterprise. These devices offered little in the way of enterprise policy management or centralized configuration, and posed new threats to information security due to their enhanced

 

capabilities. AHS decided to address these new security risks by implementing additional security controls for HIPAA compliance.

In 2010, tablet computing devices began to revolutionize the way people experienced technology. AHS was not immune to this disruptive technology and quickly attempted to embrace it in its Midwest regional facilities. At the same time, the rapid adoption of health IT put computers in the hands of clinicians where higher levels of clinical effectiveness and patient safety can be realized. The initial attempts by AHS to support this adoption resulted in discovering that the computing devices available thus far have not been well adapted to the clinical environment. Issues of battery life, portability, and ease of use have fallen short of expectations. However, the phenomenal rise in the popularity of tablets has since created an opportunity to get more user-friendly and secure computing devices in the hands of physicians who have accepted the technology with open arms.

## Deployment Challenge

In 2009, AHS began an ambitious schedule to implement computerized provider order entry (CPOE) across 39 hospitals. This aggressive timeline required that clinicians quickly complete rigorous training in order to utilize the system effectively. Physician training is critical to the successful roll out of any CPOE initiative. It became apparent that an incentive would be needed to motivate clinicians to complete the required training modules in the timeframes needed for successful implementation. The popularity of the iPad made it a natural choice for this incentive, as it would have future clinical uses as well.

Every physician that completed their CPOE training received an iPad. However, AHS had not yet developed technical standards or security processes for clinical utilization of iPads. Some of the existing technology that had been implemented for secure email with iPhone and Android devices was utilized, but AHS quickly learned that tablets were a very different type of device. A different approach was needed. Although AHS is still learning and adapting to these devices, the organization recognized that mobile computing devices reflect the future of the success of health IT. AHS determined that using a single, corporate owned device for accessing data was

 

no longer acceptable. Finding a way to embrace these new devices, while maintaining compliance with HIPAA and patient privacy, became their goal.

## Technology Utilized

The first challenge to address was how employee-owned devices could be identified and connected to the network. These mobile computing devices could not be directly attached to the hospital network, as there was no acceptable way to verify that the devices had been secured or to regulate the transfer of ePHI data to the device. In addition, the devices were not forced to utilize a secured profile for encrypting data copied directly to the device.

AHS proposed a solution that utilized the existing guest wireless network for these employee-owned devices. However, this presented additional problems. Clinician network traffic would be intermixed with internet traffic from patients and guests. This allowed for "man-in-the-middle" network attacks, as well as very low prioritization of clinical traffic. It soon became apparent that a completely separate, "provider" network needed to be established just for these devices. This provider network required each device to be registered by its mobile computing device (i.e., MAC) address before allowing access to this secured wireless network. The process required the physicians to work directly with the IT department to physically register the device. However, despite this additional layer of cumbersome and resource intensive support, it provided an appropriate level of information security.

The software that was utilized to secure email on the AHS iPhone and Android devices was made available to iPad users as well. This software did allow for the secure storage of electronic communication on the iPad as well as remote management capabilities. However, the user experience was found to be lacking, as the messages were contained in a separate application in lieu of integrating with the native iPad/iPhone/Android email application.

## Application Access

Once the mobile computing devices were connected to the provider network, AHS faced its next challenge - how to deliver applications securely to the iPad. AHS had previously implemented a thin client model for application deployment. This model required that the client application be

 

installed on the iPad in order for the device to access these applications, and provided a high degree of security, as no data was left on the device itself. There was little risk if the device was lost or stolen since nothing of value was left on the device. The communications channel was encrypted in order to prevent eavesdropping and protect data in motion. The system also allowed for the utilization of dual factor authentication.

AHS discovered some drawbacks to mobile computing device application access using the thin client model. Windows applications do not take advantage of the native hand gestures or other iPad features that users purchased the device for in the first place. Simple procedures such as double-clicking were not intuitive and interfaces were not scaled appropriately for using touch based input. Some applications required resolutions greater than what the iPad could display, which caused scaling and severe loss of functionality. Applications that were deployed in this way were required to be tested for these issues prior to deployment.

In 2011, AHS is deploying applications through web services as another avenue for iPad/iPhone/Android users to access clinical applications. This approach also meets security requirements as no data is left behind on the device and all communications are encrypted. It also allows for the utilization of the native touch gestures and provides an intuitive user interface. Although most web applications are not as feature rich as their thick client alternatives, AHS has found that this limitation has been offset by the additional ease of use.

## Lessons Learned at AHS

1. Mobile computing devices are changing too rapidly for IT to test and certify each one.
2. Mobile computing device strategies need to focus on alternative application delivery.
3. Security requirements need to be met, but most controls will impact ease of use.
4. Application vendors have not caught up with developing native applications for these devices. Native applications will drive adoption even further.
5. There are drawbacks to offering Windows applications through thin clients on mobile computing devices.
    a. Android support is more difficult due to different versions supporting certificate management.

 

   b. Windows applications are difficult to use in a touch screen environment.
   c. Thin clients require constant connection which can reduce device battery life.
6. Dedicated, secure wireless networks may be too resource intensive to support.
   a. IT staff needs training on different devices to provide support for connectivity.
7. Users may not be familiar with the operation of these devices and will need additional training. Being able to successfully manage multiple devices may only be achieved with increased vendor device support.

## Summary

Mobile computing devices are the future of healthcare computing. However, the homogeneous computing model that has been used successfully in the past needs to be expanded to support these new devices. Mobile computing devices offer many security capabilities not found on more complex thick clients, but still lack some of the management tools necessary for information security and HIPAA compliance. Third-party tools, although still in the early stages of development, have recently become available to provide additional levels of management. It is important that health IT and security professionals acknowledge and embrace these devices in order to maintain a competitive advantage for their organizations.

 

## Contribution Acknowledgement

The Security of Mobile Computing Devices in the Healthcare Environment White Paper was developed by the HIMSS Mobile Security Work Group.

James Brady, Chair
Hawaii Health Systems Corporation

Sharon Finney, CISSP, CISM
Adventist Health System

Reid Oakes
Oracle Healthcare

Connie J. Sadler
Lucile Packard Children's Hospital at Stanford

Dennis M. Seymour, CISSP, PMP
Ellumen, Inc.

Beau Woods
Dell SecureWorks

Special thanks to Adventist Health System and Joseph C. Granneman, CISSP, CSCS, CNE, MCP, CCA, Regional CIO, Adventist Health System - Information Systems, for participating in the case study.

 