Mobile Security Toolkit

Considerations for Employee-Owned Mobile Computing Devices

By Dennis Seymour, CISSP, PMP

Background

In the past few years, the technology landscape has been drastically changed by the introduction of mobile computing devices. Mobile computing devices, primarily tablets and smartphones, are a new type of platform in healthcare operations with most having slightly less power than laptops and workstations, but clearly with more functionality and connectivity. The popularity of mobile computing devices 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, where the devices potentially bring lower costs and higher quality of service.

Frequently, healthcare organizations are faced with the challenge of when and how to deploy mobile computing devices. Many times individual employees have their own devices that they would like to connect to the healthcare organization's network. The security issues and associated policy challenges for the healthcare entity involved in determining whether to allow personally-owned devices to connect to its network have both technical and legal aspects.

Roger Baker, Chief Information Officer for the Veterans Administration (VA), was recently interviewed for *HealthcareInfo Security* magazine[1]. In his interview Baker stated "We're establishing what it is we need to have the user sign, relative to their personally-owned device, that will ensure, for example, that I have the right to wipe any VA information off of it at my discretion ... and ensure that I have the right to access the device to review it as needed." With respect to the use of mobile computing devices, Baker went on to say "I would expect to see, in the long run, a phase out of desktop computers and a phase in of mobile devices."

Purpose

This white paper will provide recommendations to healthcare organizations that are considering the use of employee-owned mobile devices to access an organization's network resources and/or patient healthcare data. Our intent is not to deep-dive into the overall process for securing mobile devices, but only to identify what minimum steps the organization should take when considering the use of these devices on their networks.

[1] http://www.healthcareinfosecurity.com/interviews.php?interviewID=1272

Drivers

With respect to mobile computing devices, many consider accommodating employee-owned devices as a "fact of life" for organizations in all industry sectors worldwide. Employees like the portability, ease of use, connectivity, etc., and often own such devices before the organization itself can deploy and provision them. They often "volunteer" to use them at work, as they view them as easier to use than some of the organization's other computing resources.

The Information Technology (IT) and information security staff in the healthcare organization are concerned with the security of the network, IT resources and the confidentiality of patient medical data. As such, they must proactively and carefully consider the risk implications of allowing these types of devices. If they choose to allow use, they must put in place the appropriate policies, procedures and security controls.

First Steps

So what can information security staff in the healthcare organization do to minimize the risks involved in enabling staff members to use personally-owned tablets, smartphones, and other mobile computing devices for business purposes?

1. Conduct a survey of employees to understand the types of personally-owned devices employees may want to use for work-related tasks
2. Develop risk assessment process for these devices, including user input to the process
3. Apply the same or similar policies and security controls to these personally-owned devices as you apply to corporate-owned devices
4. Develop a legal user agreement with those who use personal devices for work-related purposes, and
5. Develop an employee education training and awareness program

Weighing Risks

Permitting the use of personally-owned devices to access the organization's network, applications and computing resources brings risks. The devices are easily misplaced, which can make any data stored on them vulnerable. The organization must require security controls, such as encryption and remote wipe capability and ensure that training is provided to users to understand the requirements established.

The organization should consider the use of employee personally-owned devices as part of their overall security risk assessment and risk management processes, just as they would any other type of remote access. This includes consideration of the risk posed by the technical capabilities and/or limitations of the device, as well as possible employee actions. The HIMSS Risk Assessment Toolkit provides resources for conducting a security risk assessment.

Legal User Agreement

Organizations should require users to sign a document relative to use of their personally-owned device for work-related purposes that will ensure, for example, that the organization has the right to wipe any organizational data off of it at management's discretion, and to ensure that the organization has the right to access the device to review it for organizational data as needed. The organization must develop this document and require users to agree to it prior to the granting of access to data/network by the device. A sample Mobile Device User Agreement is available in the HIMSS Mobile Security Toolkit.

Security Controls

Whether the device is organizationally or employee-owned, the implementation of specific security controls on mobile devices must be part of the process. The following minimum controls are recommended:

1. Implementing strong password controls, including:
   - Minimum password characteristics (number and types of characters);
   - Password history to prevent re-use of prior passwords;
   - Passwords that expire and periodically are required to be reset;
2. Screen settings should include contact information for the owner that is viewable before login;
3. Inactivity time out;
4. Lock out after set number of failed attempts to log on;
5. Remote wipe (i.e., deletion of organizational data) capability if the device is compromised;
6. Encryption, if devices are capable of employing it, and
7. Employee education and awareness.

Managing Devices and Data on those Devices

Organizations must develop a policy for the management strategy of these devices, including building in flexibility for device types, investing in mobile device management tools or services, developing procedures for obtaining mobile devices, applications, and services, and considering the level of effort required by support staff, service desk staff, and administrators to support these devices and the applications necessary to provide access to the data.

Local Storage of Data or View Only Access

Recent data shows that a significant number of breaches of Protected Health Information (PHI) reported to the Department of Health and Human Services are related to lost or stolen portable computing devices.[2] One resulting consideration for healthcare organizations is whether to allow storage of sensitive information on personally-owned devices. Allowing such data to be stored on these devices increases risk to the PHI and this must be considered as part of the security risk assessment.

The two policy options to consider are “view only access” from these devices, equivalent to "not to store", and allowing local storage of data. As part of the risk assessment, the organization should consider if storage of PHI on portable devices is part of the normal workflow for the organization and is absolutely necessary for that workflow. If at all possible, the organizations should disallow this practice, thereby reducing risk to the PHI through policy and procedural means. If local storage is allowed as an option then data encryption must be seriously considered as a mandatory security control.

Where PHI is involved and the decision to encrypt this data has been made, an issue arises that some of these devices cannot accommodate full disk-level encryption. To address this issue, some organizations are only allowing applications and devices that permit at least some level of encryption and allow the use of software applications that provide the ability to conduct a remote wipe of organizational data in the event of suspected loss of a device.

[2] See: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Screen Settings

The device should require a form of access control. This can be a PIN, pattern, or software application, and could even be biometric. The intent is security for the device, not authentication to the network or applications used by the organization. This should, where possible, include the ability to lock the device after a set number of failed login attempts.

The device should also be configured to show the owner’s contact information without login and include at least name and phone number. This information can help someone return devices to their rightful owners, while also preventing unnecessary remote wipes.

Remote Wipe Capabilities

Remote wipe capabilities that permit management to delete data from lost or stolen devices can add an extra layer of risk mitigation. For a remote wipe to work however, a device must be registered before it gets lost. Users can register their devices through the manufacturer’s website and sometimes through third-party security applications as well. Once the device is lost or stolen, it’s too late to register the device -- and it could be too late to save the data. It is important to note that this is not necessarily a control that can always be relied upon since an unauthorized user of a device may remove or replace the SIM card, which would prevent the remote wipe from being successful and make any unencrypted data accessible to the unauthorized user.

Encrypting Mobile Devices

It is important to encrypt sensitive data on mobile devices, whether it's owned by the employee or the organization. Only after entering the correct PIN, pattern or password will the person using the device be able to access its data. The encrypting of data locally should be mandatory to allow the organization to meet regulatory requirements such as HIPAA, Sarbanes-Oxley, and other legal requirements.

Employee Education

Education and awareness training is key to ensuring that users understand the organization’s mobile device security policy. Employees should receive training on the organization’s policy and user agreement and the security controls the organization will place on the use of these devices. Additional training topics should include such areas as legal requirements, incident reporting, reporting of lost devices, how to properly back up personal information (music, photos, etc.) stored on the device in case the organization must conduct a remote wipe due to lost device, and general training on application use, encryption, malware software and related topics. Clearly the organization must hold the employees accountable for their actions and those possible employee actions must be considered during the risk assessment process.