Technology Now
Timely Topics for Academic Medical Centers
a product of the AAMC's Group on Information Resources (GIR)

Group on Information Resources
GIR

AAMC

Consumer Mobile Device Security Management

October 2011

By Kenny Chu, Senior Director, IT Security, The Mount Sinai Medical Center, Alexander Grijalva, Information Security Compliance Manager, University of Medicine and Dentistry, of New Jersey (UMDNJ)

Consumer Mobile Device

The mobile market is rapidly evolving, as well as the threats and vulnerabilities affecting mobile devices. Selecting what platform to support (if not all) will depend on the objectives of each institution and the services it will make available to its personnel.

The consumerization of enterprise information technology poses challenges to the security management of information accessible or stored on mobile devices, especially, but not limited to, information protected by HIPAA and FERPA.

Strategic Considerations

- Consider the ability of the mobile platform to support password protection, device encryption (which currently satisfies the HIPAA Safe Harbor provision), and remote wiping.
- Determine whether users will manage their own device security (including personally owned devices) or if the institution will mandate a managed device security policy.
- Determine whether policies are enforced by administrative controls (user attestation form) or using technical controls such as Mobile Device Manager (MDM) software.
- Develop and implement a mobile computing policy that clearly establishes user responsibilities and the institution's expectations regarding protection of its information stored and accessible on mobile devices.

Advantages

- The large number of devices have form factor and options that suits most users' personal preferences
- Reduces the number of communication devices some people carry
- May shift cost from the institution to the individual
- Wireless options allow devices to connect to high speed cellular and/or Wifi networks
- Broad range of applications are available to support both educational and clinical activities

Disadvantages

- Sensitive information can be stored on consumer devices
- Growing malware attacks targeting mobile platforms
- Exploitable operating system vulnerabilities
- Inventory management

Resources

Apple, iPhone in Business, iOS 4 Education Deployment Guide
Gartner, Critical Capabilities for Mobile Device Management.
Android, Android 3.0: Five Features Your Enterprise IT Manager Will Love
Soundcomber: Proof of Concept Trojan Indiana University

Technical Safeguards

The technical safeguards described below are supported by the five major platforms for mobile devices – Apple iOS, Google Android [1], HP WebOS [2], Microsoft Windows Mobile, and Research in Motion Blackberry OS[3]. Some features require cell service or network connectivity.

Notes: [1] Encryption capabilities on Google Android varies depending on the version. [2] HP has announced that it will no longer manufacture WebOS hardware and is looking to sell or spin off WebOS. [3] Blackberry uses a different OS on their tablets (QNX).

Encryption
Prevents unauthorized users from reading the data stored on the mobile device. Third party email only encryption solutions may be available to support devices that cannot enable full device encryption.

PIN lock and remote wipe
Resets the device to factory default after a defined number of failed attempts to unlock the device or if a remote command is received by the device.

MDM
Mobile Device Management systems facilitate the central control of device security policy that include the use of password, device encryption, remote wipe commands, Virtual Private Network (VPN) requirements, and defines permissible applications. Many mail synchronization systems and VPN solutions include basic MDM functionality.

VPN
Virtual Private Networks create a secure connection between the mobile device and the institution's internal network.

Remote Desktop Access / Virtual Desktop
The mobile user views and remote controls a desktop session hosted on an institution's computer. This avoids having to copy data to the mobile device.