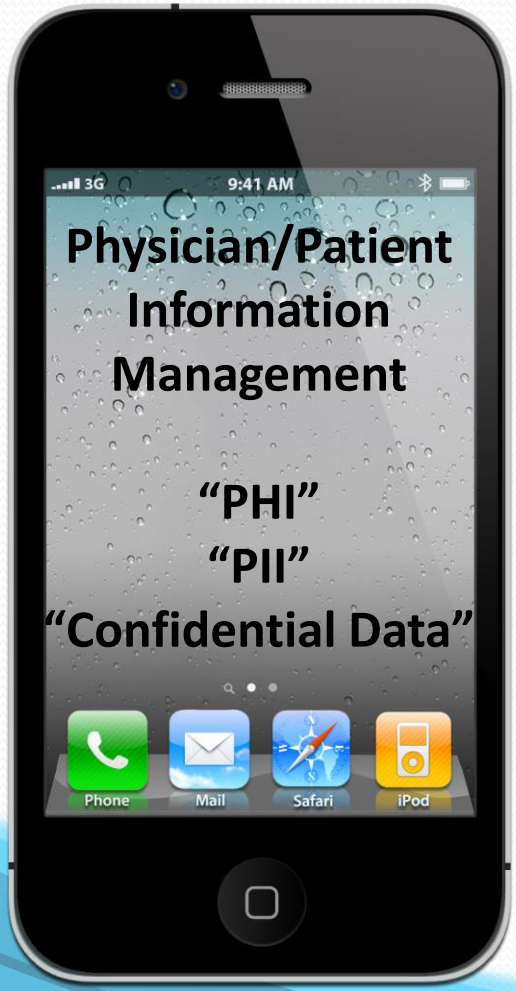

PHYSICIAN'S PRACTICE

Emerging Issues – Securing Information on Smart Devices

Sajay Rai CPA, CISSP, CISM
Securely Yours LLC

May 9, 2013

Securely Mobile

A division of Securely Yours

Securely Mobile

Security in the Palm of your hand ™

iOS Security Features

Data protection

Hardware Encryption: Every iPad device has a dedicated AES 256-bit crypto engine built in that is used to encrypt data on the device.

File Data Protection: Apple uses a technology called “Data Protection” to further protect data stored in flash memory on the device.

Encrypted Backups: When an iPad device is backed up to iTunes, it can be encrypted to prevent access to information stored in the backup.

Effaceable Storage: The “Erase all content and settings” option in the Settings menu destroys all the keys in Effaceable Storage, making all user data on the device cryptographically inaccessible.

iOS Security Features

Network protection

Wi-Fi protection: iOS devices supports industry-standard Wi-Fi protocols, including WPA2 Enterprise, to provide authenticated access to wireless corporate networks. WPA2 Enterprise uses AES encryption.

Internet protection: Native internet Applications such as Safari, Calendar, Mail, etc. automatically use SSL/TLS to enable an encrypted communication between the device and networks.

Built-In VPN: iOS features a built-in VPN client to securely connect to Cisco IPSec, L2TP, and PPTP VPN servers right out of the box

iOS Security Features

Application protection

Mandatory Code Signing: iOS requires that all executable code be signed. Built-in apps like Mail, are signed by Apple. Third-party apps must be signed using a certificate from the iOS Developer Program.

Application Sandbox: All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device.

System Software Personalization: All iOS devices prevents the installation of unauthorized operating system and prevents iOS from being downgraded to a less secure version.

- Step 1: Define the smart device use policy. Consider the following:
  - Corporate devices Vs. employee devices
  - Separation of personal Vs. corporate data on device
  - Personal use or only corporate use? Can you play Angry Bird on your device?
  - Agreement with employee to abide with corporate security policies (e.g. remote wipe, or record of their phone calls may be viewed by corporate)
  - Would confidential data be allowed on smart devices and how it will be monitored and controlled?
  - What type of smart devices will be allowed? Apple only? Android only? Or limit by operating systems?
  - How are you going to manage the backup?
  - Would you want the device to connect to corporate network?
  - Which apps would you like to deploy? Corporate apps? Own Marketplace?

- Step 2: Design the smart device IT architecture. Consider the following:
  - Cloud based solution vs. internally deployed
  - Hosted vs. self supported
  - Number of devices supported and scalability
  - Changes to the current IT architecture

- Step 3: Define the smart device security policy and security architecture. Consider the following:
  - Password Policy control
  - Encryption requirements
  - Port Control (WiFi, bluetooth, camera)
  - Remote lock/unlock/wipe
  - Asset tracking
  - Device configuration (VPN, Email, WiFi)
  - Delivery and control of applications to the device
  - Blacklisting/Whitelisting
  - Audit and Monitoring

- Step 4: Deploy the IT and security architecture and provision the device.
  - Provide emails of device owners to SM
  - SM sends a self-registry link to users
  - Users enter the registry information and obtain credentials
  - SM downloads the security policies on the device
  - Device is ready for use

- Step 5: Enable Email, Calendar and Contact information on the device.
- For ActiveSync/Lotus Notes users
  - Combine ActiveSync/Lotus Notes capabilities with selected solution to implement email policies
  - Is the corporate anti-virus updated for mobile virus checks? Or should virus scan be performed by middle-server?

- Step 6: Enable deployment of corporate mobile applications on the device
  - Typically browser-based apps are enabled
  - Whitelisting/blacklisting policies are deployed?
  - Authentication protocols?

- Step 7: Allow the device to access corporate network
  - Remote Access Policy?
  - VPN connection?
  - Encryption policy?
  - Authentication protocols?

- Step 8: Manage regulatory compliance and governance requirements
  - HIPAA
  - SOX
  - PCI
  - ITIL

- Step 9: Manage reports and dashboard
  - Executive and detailed dashboard
  - Customize reports

- Step 10: Manage monitoring and provide audit support
  - Real time vs. offline analysis
  - Audit support for smart devices