Sprint
Mobility Management Partner

VISION
Wireless Mobility Management

Mobility Management

Current Challenges and Best Practices for Increasing Efficiencies, Reducing Costs and Enforcing Policy

September 27, 2012

Sponsored by Sprint and Vision
Jennifer Warren, Director of Business Development, Vision

Vision is a leading provider of Mobility Management solutions and a highly valued Sprint Mobility Management Partner.

Agenda

- *Market Trends*
- *Business Challenges and Needs*
- *Mobility Management Best Practices*
  - *Lifecycle Management and TEM*
  - *Mobile Device Management (MDM)*
  - *BYOD Program Management*
- *Benefits*

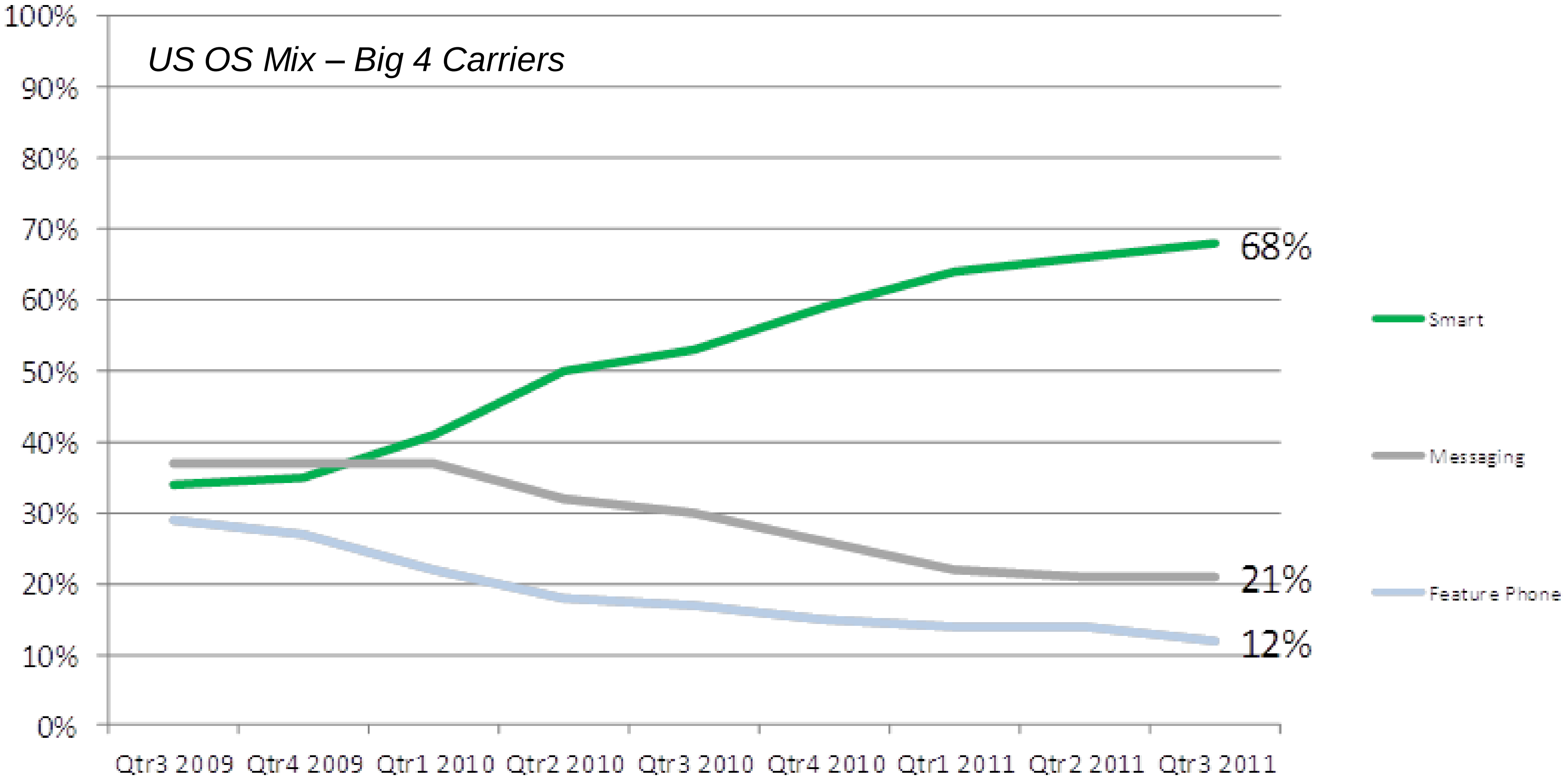
Mobile Device Trends in Healthcare

- *Wireless expenses account for nearly 35% of total telecom spend and are increasing*
- *Nearly half of business users now have smartphones*
- *Healthcare organizations support, on average ,2.5 mobile operating systems**
- *62% of Healthcare organizations are planning to deploy tablets**
- *Deployment of mobile business applications is increasing by 50% per year*
- *74% of Healthcare organizations have a wireless policy**
- *Nearly 50% of Healthcare organizations face security risks due to lack of controls to* <u>*enforce*</u> *policy*
- *Increased pressure to support BYOD*
  - *Physicians want to use their personal mobile devices for work purposes*

Source: AOTMP 2012

Smartphones Now the Norm

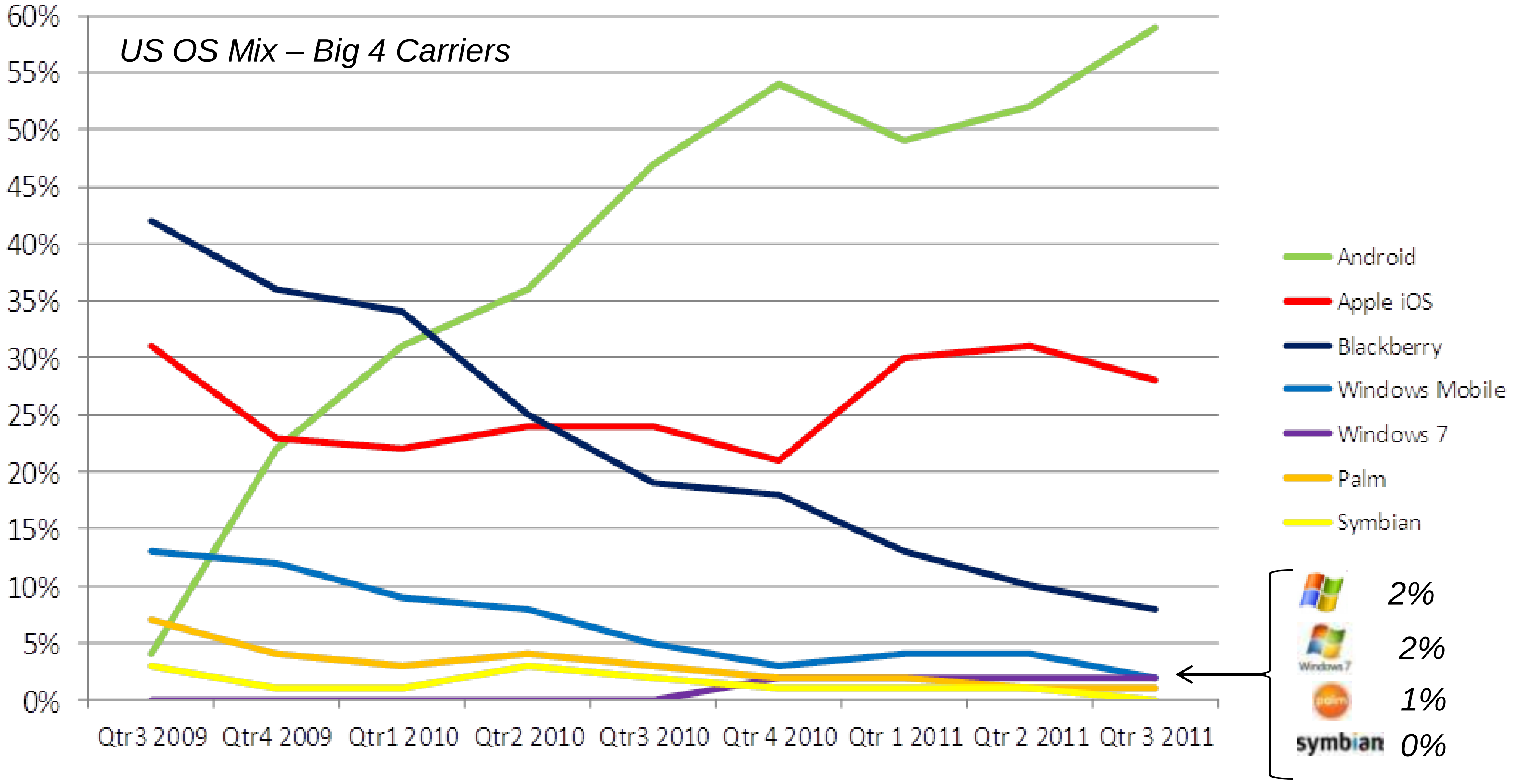
Smart devices inherently create greater security risk, simply based on the amount and type of information that can be stored locally



Source: NPD Group

Rise of iOS and Android

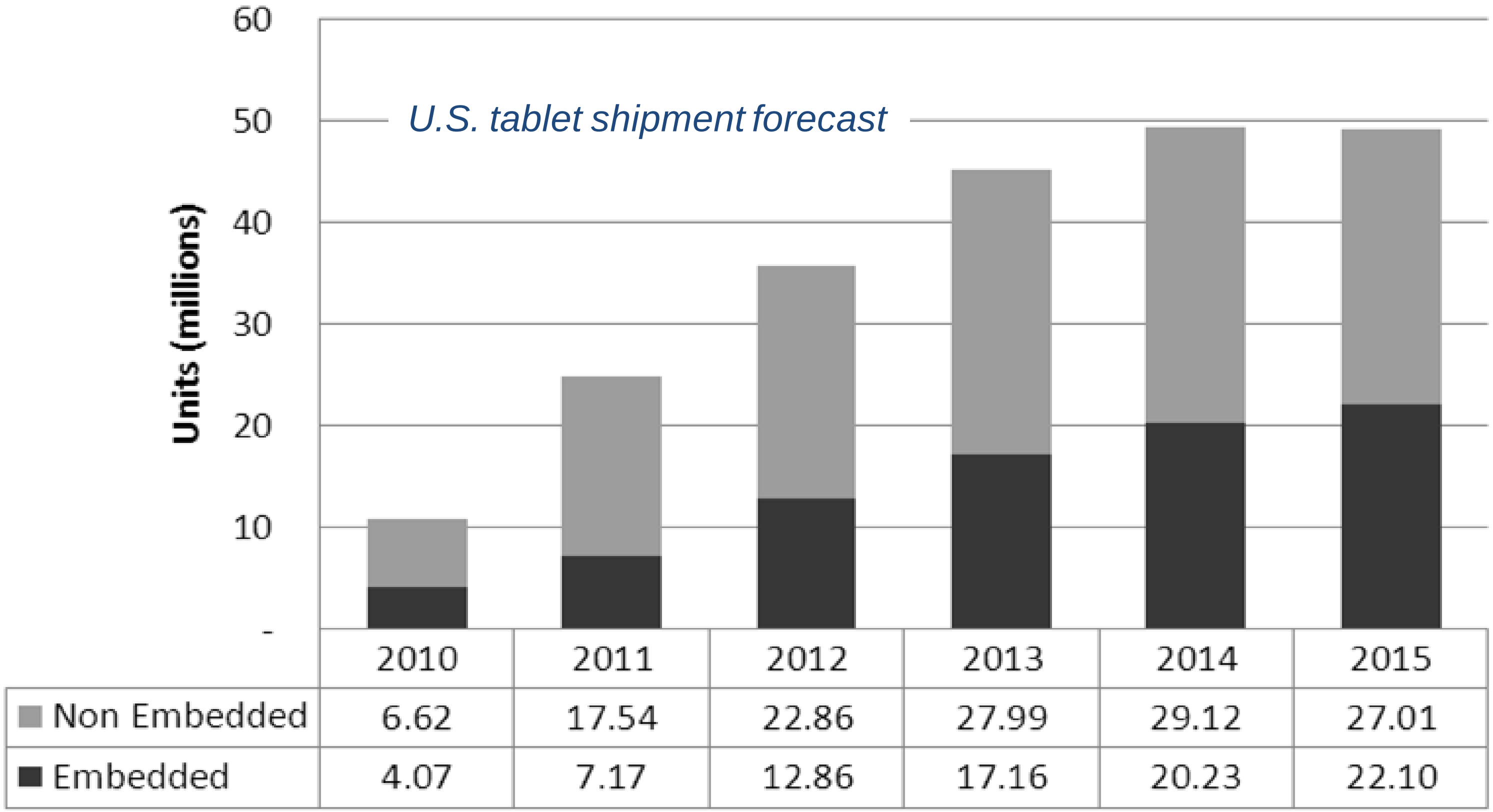
As Blackberry and Windows Mobile decline, Android and iOS, initially developed for the consumer market, penetrate the Enterprise



Source: NPD Group

Tablet Usage Growing Dramatically

The proliferation of tablets creates an incremental device to manage as an endpoint on the Enterprise network

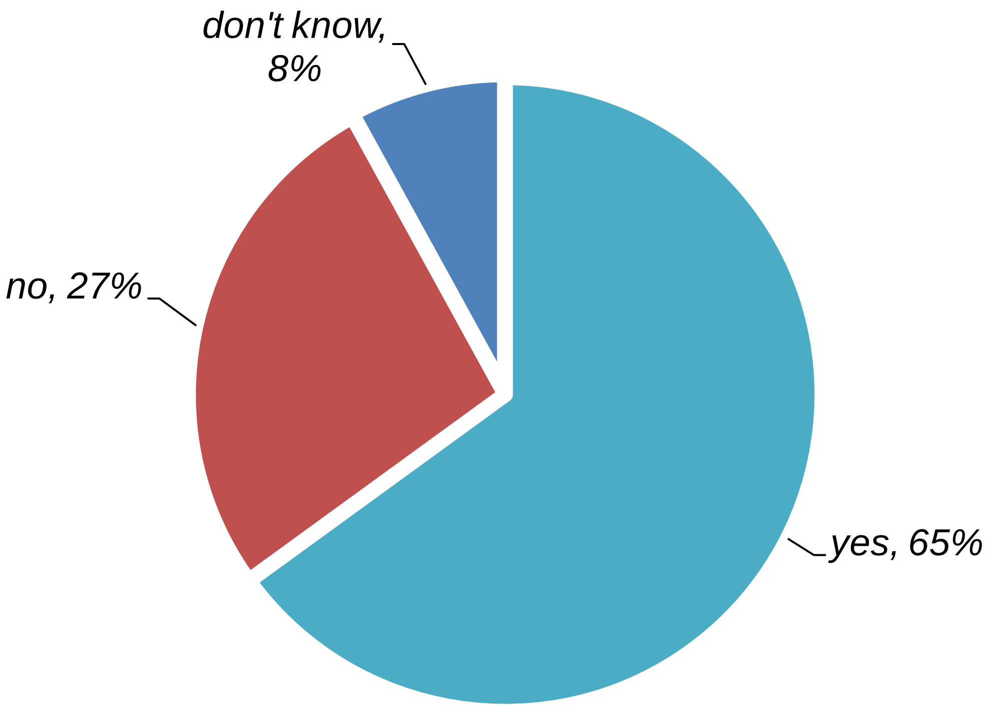


	2010	2011	2012	2013	2014	2015
■ Non Embedded	6.62	17.54	22.86	27.99	29.12	27.01
■ Embedded	4.07	7.17	12.86	17.16	20.23	22.10

Source: ABI Research

Shift toward BYOD

Shift in purchasing models moving from traditional company-owned devices toward a variety of “bring your own device” options



Q: Do you predict an increase in the percentage of employee-owned SmartPhones and Tablets accessing business resources?

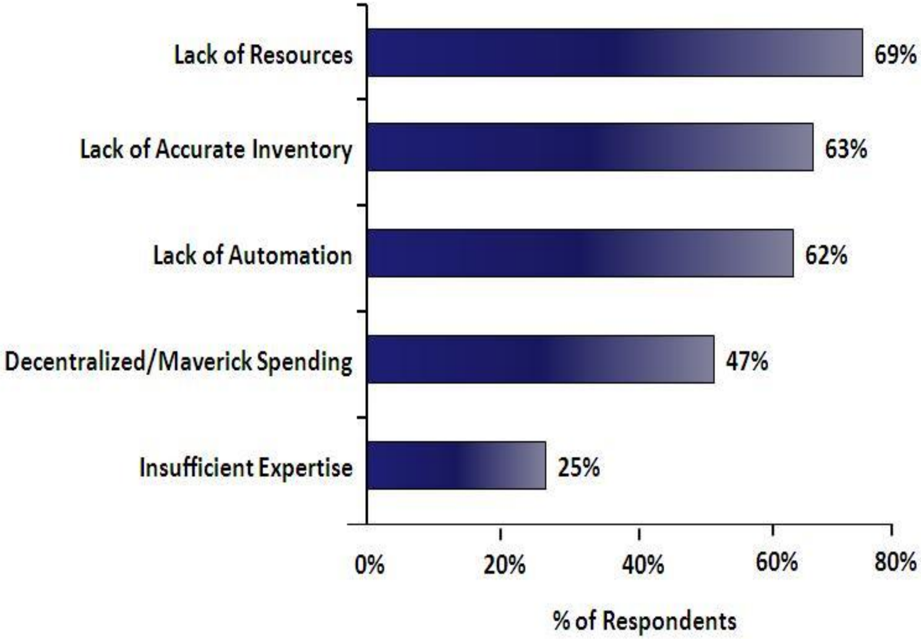
Source: InformationWeek Mobile Device Management and Security Survey, August 2011

Top Mobility Management Challenges

Supporting these rapidly expanding mobile environments creates challenges

Increasing complexity

- *New device types*
- *Multiple operating systems*
- *Multiple carriers*



Managed solutions

- *Businesses of all sizes, across industries, are embracing outsourced professional and managed services*
- *These services can reduce costs and complexity while enhancing the impact and benefits of mobile investment*

Source: AOTMP

Mobility Management Best Practices

Device Lifecycle Management and TEM

- *Custom portal – your plans, your devices, your policy*
- *Track orders to fulfillment*
- *Move, add, port, swap, upgrade*
- *Track assets to users*
- *Optimize plans and pools*
- *Allocate costs & usage*
- *Identify misuse & enforce policy*
- *Manage invoice & remittance*

Mobile Device Management and Security

- *Enforce passwords*
- *Lock a device*
- *Remote wipe device and/or SD card*
- *GPS / location tracking*
- *Real-time device statistics*
- *Restrict access to corporate resources*
- *Create & enforce policies by device type or user group*
- *Push required applications*
- *Encryption*

B.Y.O.D Program Management

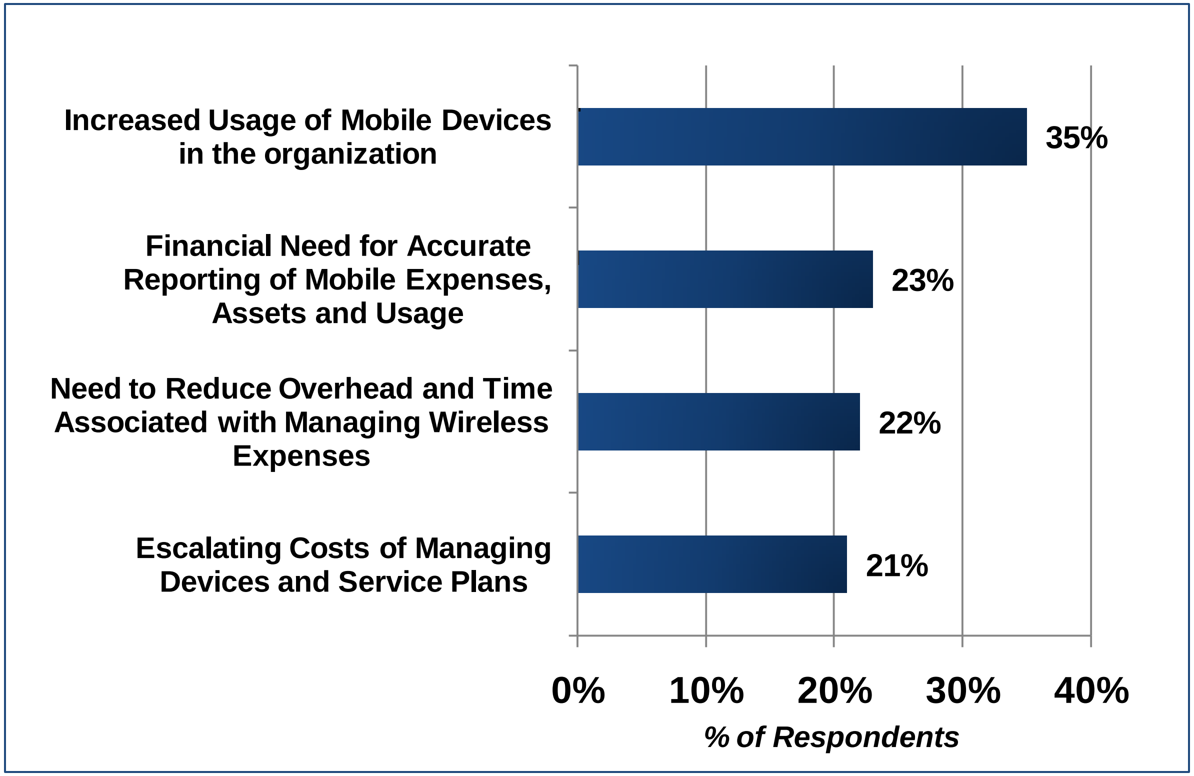
- *Register users & track connected devices*
- *Communicate BYOD policy and track user acceptance*
- *Connect device to corporate email & other resources*
- *Secure devices with MDM*
- *Stipend management*

Wireless Help Desk

Premium Web Tools

Across your whole mobile environment, regardless of mobile operator

Top Pressures for Wireless TEM



In-House Approach versus 3rd Party Solutions

- *In-house programs average 2.4 Full Time Equivalents (FTEs) per 1000 devices vs. only 0.8 FTE for 3rd party WMM/TEM solutions*
- *In-house programs average 0.9% over budget vs. 3rd party solutions which average 1.9% under budget*

Source: Aberdeen Group, Controlling Wireless Expenses, Sept 2010

Benefits of Lifecycle Management & TEM

Tight controls, efficient processes and optimal end user experiences

Control + ***Performance*** = ***Results***

Control

✓ Increase Visibility

→ Know your Users

→ Know your Devices

→ Know your Plans

✓ Centralize Management

✓ Enforce Wireless Policies

Performance

✓ Simplify Multi-Carrier Management

✓ Employ Proven, Best Practices

✓ Streamline Business Processes

✓ Improve End User Experience

✓ Analyze & Adjust for Continual Improvement

Results

✓ Optimize Wireless Spend

✓ Reduce Costs

✓ Save Time

✓ Improve Operational Efficiency

✓ Increase End User Productivity

B.Y.O.D. Market Drivers / Expectations

Employee preference for device make/model	• Employees/physicians don’t want to carry 2 devices
Stabilize increasing wireless costs	• Offload capital expense of equipment (device) to employees • A “Stipend” eliminates the “Moving Target” of Wireless Costs
Enhance productivity by extending access to broader user base	• e.g. email, calendar (appointments), contacts, patient data
Limited internal resources for Help Desk & administrative support	• Desire to shift burden of support to wireless carriers

B.Y.O.D. Challenges & Considerations

Not appropriate for all employees or all mobile devices

- Risk profiles & regulatory environment must be carefully considered
- Some applications may always require corporate-owned devices

Legal and security concerns

- Physicians who deal with sensitive data such as Patient Healthcare Information (PHI)
- Cost of MDM solutions are needed for multi-OS management to secure devices, manage policy & protect sensitive corporate data (e.g. remote lock/wipe, etc)

IT support costs and administrative burden does not go away

- Corporate IT department still remains first point of contact for end user
- More device makes/model and mobile OS types to be supported
- Employees/physicians must rely on carriers for support of IL device & rate plan; can cause decreased user productivity

BYOD in Healthcare

- *83% of healthcare IT professionals allow iPads on their enterprise networks*
- *65% support iPhones and iPod Touch devices*
- *52% of hospitals support personal BlackBerry devices (more than most industries)*
- *46% of IT professionals allow enterprise use of Google OS on personal phones or tablets*
- *58% of respondents are using virtualization technology to access applications on iPads*
- *8% of respondents provide complete access to hospital network on personal mobile devices*
- *24% of respondents provide at least limited access to hospital applications*
- *60% reported that their organizations allow EHR access on employees' own devices*

Aruba Networks: Survey of 130 IT professionals surveyed in February 2012 at the HIMSS12 Healthcare IT Conference in Las Vegas, NV

Mobile Security Policies to Consider for HIPPA Compliance

BYOD in the Healthcare Industry

- **Lockouts** – set devices to lock after a specified number of failed attempts as well as a specified amount of time to keep data protected during downtime. Lockout should require password reentry.
- **Device Lock** – require minimum characters and password reset on reoccurring basis.
- **Device Authentication** – mobile device login to verify user identity when remotely connecting to the corporate network.
- **Remote Wipe and Tracking** – mitigates risk by remotely wiping, locking, or locating the device if it is lost or stolen, an employee leaves the organization, or there is a virus or breach.
- **Email** – require segmentation of Healthcare Email and Personal Email systems.
- **Encryption** – encrypt all data at rest and in transit, including backup data.
- **Applications** – all applications that create, store, access, send or receive PHI must meet HIPAA security standards.

Mobile Security Policies to Consider for HIPAA Compliance

BYOD in the Healthcare Industry (Continued)

- **Wireless** – require the use of SSL when using digital cellular to connect to the network and if not using one of the organization's carriers. Require a password or PIN for Bluetooth connectivity.
- **Updates** – security updates, patch management, and using the most recent OS available should be standard to keep up with evolving threats.
- **File Sharing or Backup** – use a secure file transfer tool or protocol (SFTP) when sending electronic health information and discourage use of DropBox™ or similar services.
- **Device Disposal** – put in place a process for securely destroying or deleting PHI when upgrading or disposing of a mobile device.

Thank You!