WHITE PAPER

Is BYOD Right for Your Hospital?

Mobile Devices in Healthcare

Vocera Communications, Inc.
May, 2014

Key questions you should ask when considering the use of personal mobile devices in the hospital

Bringing your own mobile device (BYOD) to the workplace, once considered a radical departure for Information Technology departments, is commonplace today. Some say the trend was sparked by the debut of the iPhone®, which was embraced by consumers but not necessarily by the enterprise. Whatever the impetus, it has become abundantly clear that many employees prefer to use their own mobile devices both at home and at work.

On the positive side, BYOD programs save organizations money by shifting device costs to the employees. In addition, because employees upgrade more frequently, their personal devices tend to be more current. And, not insignificantly, allowing employees to use their own devices can make them happier and more satisfied with their jobs.

Of course, implementing BYOD does have its downsides. Given the highly sensitive data managed by hospitals, security is perhaps the number one reason that healthcare, with HIPAA requirements and the over-arching concern for maintaining patient privacy, has been slower to embrace BYOD than other industries.

Key BYOD questions at-a-glance

- Who needs a mobile device at your facility
- What types of devices and operating systems will you allow?
- How will BYOD fit into your infection control systems?
- Can you maintain data security and patient privacy with a BYOD program?
- Can you develop and enforce a BYOD policy?
- What mobile program is best for your facility?
- Can you accomodate the future of mobility?

While there is a lot of interest in BYOD for hospital applications – Gartner Group predicts the annual market for wireless health solutions will reach $1.7 billion in 2014 – most facilities have just begun dipping their toes into the BYOD waters. Hospital CIOs recognize that employee-owned smartphones and tablets can contribute to productivity and patient care, but quality and safety must be preserved. The financial ramifications alone give CIOs pause given HIPAA regulations place tighter controls over PHI with a hefty penalty of $1.5 million per data breach per incident. In addition to potential fines, data breaches involving lost or stolen smartphones and tablets that contain patient data would require a hospital to notify each patient involved, a costly and labor-intensive task.

There is no one-size-fits-all approach to BYOD, but there are some basic questions and concerns, outlined in this white paper, that hospital CIOs must consider and vet for their own institutions before making the leap.

Who needs a mobile device at your facility?

Hospitals are unique in the variety of distinct personnel required to run them effectively. The different levels of employees create an added challenge when it comes to BYOD. Here are some considerations for each type of user.

Unaffiliated physicians, early proponents of BYOD due to their high levels of autonomy and need for mobility between facilities, typically want to use their own devices. This requires that they have complete access to each hospital network they visit. How do you ensure that your data remains secure? How do you establish network security while allowing for and preserving personal data, such as photos and contacts?

Hospitals also employ staff physicians, who prefer to use their own smartphones and tablets on the job. However, since these employed physicians don't typically travel to other facilities, their access requirements may be different than those of non-affiliated physicians, and thus require a different level of network connectivity. Staff physicians' personal data still needs to be protected, especially in the event of a lost or misplaced device that would require a data wipe.

Nurses, the largest group of employees in a hospital, present yet another set of considerations. Given the proliferation of mobile healthcare apps today, nurses regard mobile devices as effective and efficient tools for patient care. They use these devices throughout the day as they care for patients, connect with physicians and other hospital departments, access records, respond to emergencies, input data in Electronic Health Records (EHRs) and look up lab and test results.

Springer Publishing, New York City:

- Approximately 1000 nurses polled
- 83% of respondents own a smartphone
- Up from 71% in 2013

However, nurses don't necessarily want to subject their personal devices to the wear and tear of daily patient care. They would much prefer to use hospital-owned equipment, whether it is a device issued for use both in and out of the hospital, or shared devices used on shift.

Another important consideration for nurses and other employed clinicians is the relationship between their union membership and a BYOD program. Labor unions are intent on defending workers' privacy rights and this extends to their mobile devices. If a hospital's BYOD policy enables the tracking and wiping of personal devices for whatever reasons, such action could run afoul of a union's consideration of workers' rights and result in legal action.

Potential users and device requirements
Unaffiliated physicians — personal devices
Employed physicians — personal devices
Nurses — hospital-owned devices
Technicians/clinical — hospital-owned devices

In addition, if the hospital has a BYOD policy, it can be considered liable for the cost of the personal device and/or plan used in support of the user's job. For example, if an employee is on a metered data plan and uses a portion of that plan in the course of their daily job, does the hospital owe them for that usage? If the hospital provides the device and allows its use outside the premises, is usage of that device at any time "chargeable" to the hospital? There have been cases in which non-BYOD hospitals were sued for "lost wages" as a result of calling off-shift personnel on hospital owned devices.

What type of device will be allowed at your facility?

In-building coverage for data is poor at best on cell networks, so hospitals use Wi-Fi to enable secure and reliable data communication within their premises. Today, there are a growing number of devices capable of using Wi-Fi to connect to a network. A hospital CIO needs to determine which devices, and more specifically, which versions of those devices, are acceptable. Conversely, if a hospital allows BYOD, but only for selected devices, what happens to those employees who own devices that are not on the allowed list?

In addition, look closely at the operating systems available to the selected devices to ensure that the communication platform and mobile apps important to your facility can be used on those systems.

Can you maintain data security with a BYOD program?

Security, privacy, and regulatory concerns:

- Data encryption
- Virus control
- Password-protection protocol
- Allowed devices, OS, and apps
- HIPAA-compliant communications platform
- Allowed personal use on hospital time
- Wipe and lock control

Security issues give many hospital CIOs pause when it comes to mobile devices. The bottom line is that no matter who owns the device, the hospital is responsible for any data breaches that occur. With hospital-owned mobile devices, a CIO has a higher level of control. Personal devices are less likely to have the required encryption and are more susceptible to viruses that could be introduced to the network through personal apps, social media, web-browsing and email.

Hospital-issued devices are typically protected by hospital security programs that are managed and updated by the IT department. It is more difficult to set and enforce policy for employees' personal tablet or smartphone use. Hospital BYOD policy must set rules regulating personal device use on company time, including taking calls, texting, and emailing. For example, an employee using a BYOD device should be allowed to call a family member or take a call from a school regarding a sick child. However, it remains a question of policy during work hours when the plan is subsidized by the hospital.

Similarly, policy should address inappropriate use of a hospital's network while on any mobile device, BYOD or hospital-owned. Hospitals, like any enterprise, do not want streamed video or objectionable content downloaded through their network.

Of course, all BYOD programs should include a rigorous password-protection protocol. But it is also essential that a hospital be able to "control" or "disable use" of a device and that employees fully understand and agree to that policy. For example, cameras can be both acceptable and clinically advantageous if used within a HIPAA-compliant communication application, but not through the regular device's operating system. However, the images must never be stored on the device, but rather saved to the server.

A security plan is essential for all hospital mobile device programs. The plan should be enforced through both a strong policy and the deployment of mobile device management software (MDM). MDM can be pricey per device, depending on how it is configured, but it could be well worth the expense given the control it provides. Emails sent from smartphones and records stored on tablets can risk serious consequences without the right procedures, technologies and oversight in place. MDM can also ensure that data is wiped in the event of a lost or stolen device.

In addition, geo-fencing and contextual MDM can secure and lock down devices based on location. For example, a hospital CIO can set up alerts so that, if desired, the camera or certain apps on a device are disabled when an employee enters the facility, or a hospital-owned device is completely disabled when it leaves the facility.

Will BYOD devices fit into your infection control system?

The use of mobile devices by healthcare workers, particularly in the operating room and the intensive and critical care units where patients are more vulnerable to hospital acquired infections (HAIs), may have serious hygiene consequences. Given that an estimated one in 20 patients is affected by an HAI, infection control is a serious concern for all health administrators. In fact, facilities are required to report their HAI rates to the Centers for Medicare and Medicaid, which uses that data as an important quality of care measurement.

It is easy to see how a mobile device that is used at the point of care could transport bacteria, viruses and other pathogens. The harsh chemicals used to wipe down most hospital surfaces and equipment cannot be used with delicate tablets or smartphones. In addition, the touch screens used on most mobile devices today are difficult to operate with gloved fingers and impossible to chemically decontaminate.

Also of concern are the specialized cases or jeweled covers used to accessorize personal devices that pose both a contamination and a foreign object risk. Hospital BYOD policy will need to consider infection control as it relates to personal devices and to include a provision that covers allowable phone accessories.

Can you develop and enforce a BYOD policy?

Most hospitals operate on the honor system when it comes to patient privacy and patient health information and employees are happy to comply. However, inadvertent breaches are a much bigger possibility with mobile devices and applications. CIOs must have a clearly defined policy for BYOD that outlines the rules of engagement and states up front what the expectations are. The policy should include minimum security requirements or perhaps hospital-sanctioned security tools as a condition for allowing personal devices to connect to hospital data and network resources.

Hospitals also face compliance and ownership challenges when it comes to data. Hospitals fall under compliance mandates that have certain requirements related to information security and safeguarding specific data. Those rules must be followed whether the data is on a hospital device or a personal smartphone.

In the event that an employee is fired, or leaves the organization on their own accord, the hospital will need to segregate and retrieve its stored data. There should be a policy in place that governs how that data will be retrieved from a personal tablet and/or smartphone.

Your BYOD policy should address the following areas in detail:

1	Acceptable devices and OS
2	Allowable apps
3	Devices and support
4	Access to hospital data
5	Reimbursement
6	Security
7	Risks/liabilities/disclaimers
8	Ramifications of violations

Do you have the resources necessary for setting up and maintaining a BYOD program?

Written policy usually isn't enough to police a BYOD program. IT departments are required to provide a higher level of oversight that can be labor-intensive and costly. For example, some facilities may find it advantageous to insist that all personal devices be individually inspected on a periodic basis by an IT department specialist to ensure that the device meets the encryption and security criteria set by the hospital's BYOD policy. These devices, some no doubt unfamiliar to the IT team, will need to be setup (configured and credentialed) by the IT department, maintained and, to some extent, supported on an ongoing basis to ensure proper use.

Another consideration is management of the applications on the device. If the hospital mandates the use of specific application/applications, how does it make sure that those apps are downloaded and maintained?

What mobile program is best for your facility?

There are three typical mobile device scenarios that hospitals should consider each with its own pros and cons. Hospitals could:

- Provide hospital-owned mobile devices for all users
- Invite all employees across the board to use their own devices
- Create a blended environment that allows a combination of both hospital owned and BYOD, depending on the type of employee

While a BYOD program can shift device costs onto the user, a hospital must determine how they will reimburse employees for their data plans, manage upgrades and control connectivity. For example, certain inexpensive data plans that employees find adequate for their personal use may have limited connectivity on a hospital campus.

Perhaps the more workable solution is a shared environment in which some employees – physicians, for example – are allowed to use their own devices, while shift employees, such as nurses, would use hospital-owned devices. The hospital devices could be chosen based on certain criteria developed in consultation with the user population, such as battery-life, ruggedness, ability to be decontaminated and hands-free operation. These devices could either be assigned to an employee for use on and off campus, or turned in at the end of a shift for secure storage and recharging.

About Vocera

No matter how you choose to move forward on developing a BYOD program for your hospital, the Vocera Communication System is designed to empower your employees by instantly connecting them to the people and the information they need right now, on their device across the care continuum. The Vocera® Communication System is a software-based solution that can run on any smart device or on the wearable Vocera Badge, inside and outside the facility. The Vocera Software Platform contains the system intelligence, including user profiles, groups, call management, and call connections, as well as the ability to interface to existing telephony, alarm and alert systems to expedite communication of mission-critical data in the hospital setting.

Can you accommodate the future of mobility?

As technology evolves, so will BYOD policies and practices. Just when a level of comfort has been reached, a new class of device or mHealth app will emerge that must be accommodated. For example, the market for wearable technology is around $5 billion today, but Credit Suisse estimates this will increase to $50 billion in just three to five years. Clearly, it is only a matter of time before hospital employees' mobile devices take the form of glasses, watches or other wearable gear. So, no matter what BYOD direction a hospital CIO decides to take, it should be done with an eye to the future. With its intuitive, intelligent software platform, the Vocera Communication System can accommodate all of the challenges you face in future-proofing your communications platform and has the expertise to help you develop the appropriate BYOD policy for your organization.

©2014 The Vocera logo is a trademark of Vocera Communications, Inc. Vocera® is a trademark of Vocera Communications, Inc. registered in the United States and other jurisdictions. All other trademarks are the property of their respective owners.

For More Information
Visit www.vocera.com,
email info@vocera.com,
or telephone 1-888-9-VOCERA.

Vocera Communications, Inc.
525 Race Street
San Jose, CA 95126
tel : +1 408 882 5100
fax : +1 408 882 5101
toll free : +1 888 9VOCERA
www.vocera.com

Vocera Communications UK Ltd.
100 Longwater Avenue
Green Park
Reading, Berkshire
RG2 6GP
United Kingdom
tel : +44 0 844 335 1237
fax : +44 0 118 945 0493
www.vocera.co.uk

Vocera Canada
8 Market Street, Suite 300
Toronto, Ontario
M5E 1M6
Canada
tel : +1 416 923 2900
fax : +1 416 923 2981

Vocera_WP_BYOD_050614