Clinical Mobility: Strategy, Best Practices and Device Selection

The success of your clinical mobility solution is tightly tied to the mobile device you select.

It's a fact that in hospitals and clinics, mobile computers help clinicians improve the quality of patient care and save lives by improving staff communication and collaboration, and by providing instant access to a wealth of mission-critical information — from real-time lab results to a change in a patient's condition or verification of the '5 rights' of medication administration at patient bedside. In addition, mobility also helps healthcare organizations comply with important governmental and regulatory safety standards, without tasking an already-overburdened nursing staff with additional paperwork — paperwork that would further reduce time spent caring for patients.

71% of hospitals identify mobile communications as a current or emerging investment priority.[1] As healthcare organizations move forward with their mobility initiatives, one of the most important decisions is mobile device selection, which will play a large part in the level of success your mobility solution can achieve.
The wrong device can frustrate users, decrease productivity, increase costs and potentially introduce safety risks. The right mobility solution will help maximize the success of your healthcare mobility deployment by increasing workforce productivity, task accuracy and return on investment (ROI).

1. Source: Healthcare without Bounds. Point of Care Communication for Nursing. Spyglass Consulting Group, July 2016

3 OPTIONS

When it comes to mobile device selection there are three options. This white paper will examine all three options, their differences and how they impact performance, productivity, and cost.

1 ENTERPRISE DEVICES

You can choose enterprise handheld mobile computers that are purpose built for healthcare environments.

2 CONSUMER DEVICES

You can choose consumer devices, such as smartphones or tablets.

3 "BRING YOUR OWN DEVICE" (BYOD)

You can allow your healthcare workers to use their own consumer smartphones and other mobile devices.

A good mobility strategy starts with a good plan.

THE FIRST STEP IN ANY MOBILITY STRATEGY IS PLANNING.
AND THE SUCCESS OF YOUR MOBILITY DEPLOYMENT DEPENDS ON THE QUALITY OF THAT PLAN.

In today's clinical healthcare environment, electronic health record (EHR) systems have become the industry standard for many patient care applications and processes because of their ability to provide accurate, up-to-date and complete patient information. Yet clinicians at the patient's bedside don't always have immediate access to this critical information which is often only available on a workstation. As a result, clinicians run the risk of making compromised decisions that can directly affect a patient's well-being.

Fortunately, clinical mobility is changing the face of patient care. No longer will clinicians have to seek out a workstation to access a patient's EHR. Instead, this real-time patient data will be accessible on mobile computing devices. When implemented properly, these devices can serve as a secure voice and data communications tool, a valuable information portal and a critical life line for hospital staff in managing alarms and alerts. Clinical mobility is also helping to improve workflow efficiencies and collaboration between patient care team members which is translating into dramatic improvements in patient care.

When it's time to integrate mobile devices into your hospital's workflows, an enterprise-wide mobility strategy is essential to averting unchecked usage of mobile devices by staff and a host of headaches for your organization. By planning ahead, you'll be able to integrate mobile devices that are purpose-built for healthcare into a centralized system — and better support your staff with fewer — and more effective resources.

Hospitals and other healthcare organizations, in particular, must contend with a daunting set of challenges when deploying mobile technology. That's why it is important to develop a carefully planned mobility strategy. To be successful, your strategy will need strong senior level leadership, commitment, funding and resources. An interdisciplinary team should be gathered — including nursing, physicians, pharmacy, IT, ancillary care, biomedical engineering and finance — to develop a vision for a common technology infrastructure that supports all staff across the organization.

5-Step Roadmap

1. Map the ways your hospital staff communicates.
2. Identify your mobile communication requirements.
3. Identify the applications and systems needed to enable key workflows.
4. Determine how you will manage alerts and alarms.
5. Determine how you want your rollout to proceed.

TODAY'S COMMUNICATION MAP

1 Map the ways your hospital staff communicates.

Carefully assess your current capabilities by surveying clinical and support staff throughout your facility to learn about the devices and applications currently in use. In many cases hospital staff is still using pagers, overhead paging systems, single-purpose voice-over Internet phones, as well as their own personal cell phones. As a result, breakdowns in clinical communication are all too common because of disparate work tools and outdated technologies.

Your mobility strategy should examine:

- Is there an enterprise-wide system?
- Does it work well for all employee groups?
- Does your system seamlessly allow for both voice and data communications?

Map the constituencies and workflows that will benefit most from mobile computing. Generally, these employee groups include bedside and procedural nurses, physicians and support service areas, such as patient transport, facility engineering, environmental services, biomedical engineering, security and food delivery.

50% of hospitals have deployed Voice-over-IP (VoIP) solutions within their organizations, improving staff communications and collaboration to help improve patient care and reduce medical errors when they are on the move.

Source: Spyglass Consulting

70% of medical errors can be traced to communication breakdowns.

Source: The Joint Commission

MOBILE COMMUNICATION REQUIREMENTS

2 Identify your key mobile communication requirements.

After looking at all the different ways your staff communicates and identifying the gaps and opportunities for communication breakdowns, you are well positioned to determine your mobile computing requirements.

Determine features as well as service level requirements and management capabilities. For example, features may include establishing an enterprise employee user group directory to help facilitate seamless team member identification via text messaging or phone calls. Service level requirements will include reliability and roaming to ensure there are no dropped calls when healthcare workers are on the move throughout your facility. And, of course, you will need to plan for technical and workflow-related security measures to ensure that employees are always following patient privacy guidelines.

Since healthcare facilities are subject to strict regulations governing data confidentiality, it is strongly recommended that hospitals consider employing a third-party mobile device management (MDM) system/provider that can assist with effecting mobile-compliant patient privacy protection and data handling. An effective MDM solution provides central control of all mobile devices in your network so that patient data is never at risk, with remote management capabilities, application control and reporting tools.

80% of nurses use standard, unsecure, HIPAA-noncompliant, bundled short messaging service (SMS) applications on their smartphones.

Source: Spyglass Consulting

To improve patient care, a recent survey found a real need for healthcare organizations to provide employees with a secure, HIPAA-compliant integrated internal communication platform for email, text messaging and voice calls that would replace outdated communication systems like pagers.

Source: "Most physician secure messaging apps not HIPAA compliant," *HealthITSecurity*, Nov. 9, 2015:
Find at: http://healthitsecurity.com/news/most-physician-secure-messaging-apps-not-hipaa-compliant

NEEDED APPLICATIONS AND SYSTEMS

3 Identify the applications and systems needed to enable key workflows.

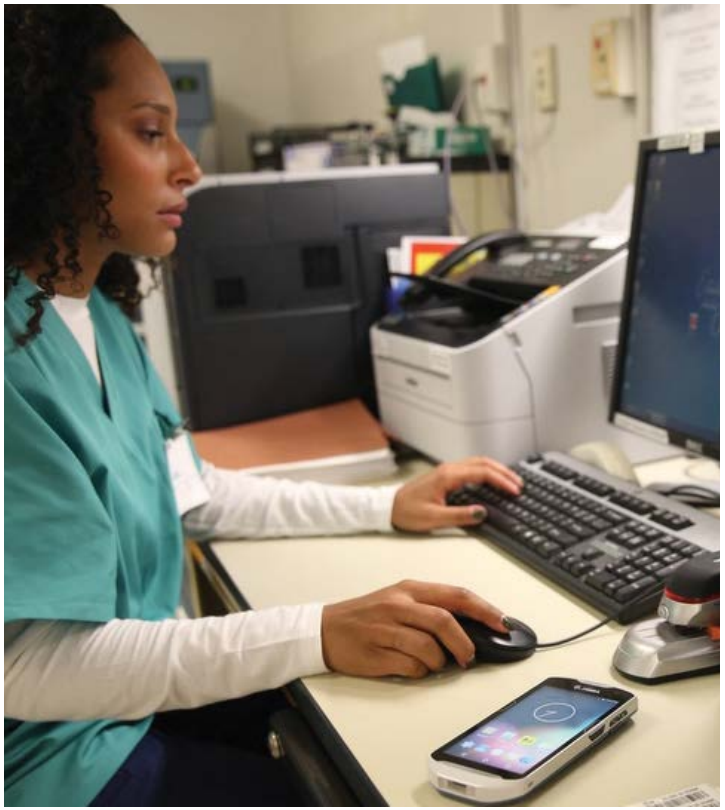
Determining the mobile technology needs of your key users also includes identifying the systems and applications they will need to access:

- Will you need to interface with your voice network systems (PBX systems)?
- Will the new mobile device need to access your hospital's nurse alert and alarm systems?
- Will your devices need to connect with an existing communications platform?
- Will you need to put a new communication platform in place?

With mobile devices, your staff will now be able to access Electronic Health Record (EHR) data and clinical workflow applications in real time. Your mobility strategy will need to provide ways to facilitate staff access to that information and improve the use and sharing of that data. Additionally you will need to determine which EHR data and clinical workflow applications will need to be enabled on staff mobile devices.

52% of nurses will use an app instead of asking a colleague for information.

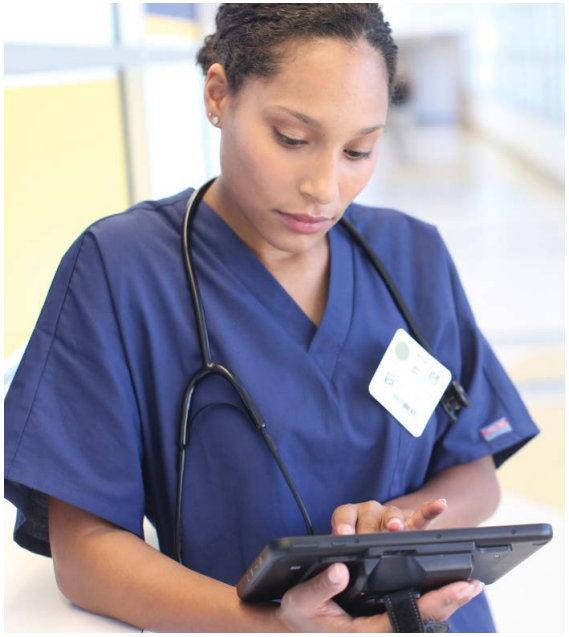
Source: InCrowd



MANAGING ALERTS AND ALARMS

4 Determine how you will manage alerts and alarms.

Hospitals are dealing with a proliferation of patient monitoring technologies. Clinicians are struggling with how to manage the constant barrage of alarms and alerts on top of their regular daily duties. While these alarms have been instrumental in saving lives, they have also resulted in one unexpected side effect: alarm fatigue.



Your mobility strategy should include plans for an alarm management program that ensures alarms are transmitted to mobile devices in a way that ensures patient safety and reduces alarm fatigue. It should include ways to differentiate and triage based on criticality.

- Do you have an application to integrate the nurse call system?
- Is that system interoperable?
- Which devices should interact with patient monitoring technologies?

You may want to consider employing a middleware company to manage the efficiency of the alarm management system.

85% to 99% of alarms are just noise generated by medical devices and don't require any action at the patient's bedside.

Source: Association for the Advancement of Medical Instrumentation (AAMI)

PLANNING YOUR ROLLOUT

5 Determine how you want your rollout to proceed.

After completing your own internal needs assessment, it's time to set some concrete short-, medium- and long-term goals and a timeframe for your mobile deployment.

Will you want to rollout your new mobile devices in a phased implementation — for example, equipping your bedside nurses on the surgery floor with devices during the first phase, followed by all nursing staff, all hospital staff, and finally the entire care continuum?

Best practices dictate a phased-in approach, beginning with voice and text capabilities to start, for example, followed by EHR applications. You will also want to factor in testing for interoperability, and providing individual training for each capability and application.

The mobility strategy that results from this due diligence should be put in writing in a living, breathing document that can be shared with your team and revised as needs evolve.

FOR MORE DETAILS ABOUT PLANNING FOR A SUCCESSFUL MOBILE DEPLOYMENT, SEE THE IMPLEMENTATION SECTION OF THIS WHITE PAPER.

Renowned Japanese Hospital advances patient care with bedside access to real-time data

Japan's Nagasaki University Hospital implemented Zebra's mobile computing solution while upgrading its electronic health record (EHR) system.

By deploying the Zebra mobile computer, which works as a mobile nursing information device in seamless conjunction with the hospital's EHR, the hospital vastly improved efficiency and accuracy.

Now, nurses can check on drug prescriptions by the bedside before administering injections or blood transfusions — and electronically record the details of the procedure with a single click. There is no longer a need to transfer records from the nurse's memory to patient files, reducing the time required for the recording process and increasing accuracy. In addition, the Zebra mobile computing device makes it possible to securely manage personal patient information.

Selecting the right mobile device

Selection criteria for healthcare organizations

In order to select the right device, you need to make sure you have the right criteria. You need to meet a wide variety of needs for different types of personnel and different departments — from healthcare workers and IT departments to infection prevention, compliance and finance. The following is a discussion of the criteria that can help you choose the right device, as well as an evaluation of how enterprise, consumer and “BYOD” devices meet each criteria.

THE ISSUE

Security is a top concern for healthcare organizations, which must comply with patient privacy protection and data security regulations that protect sensitive patient health-related information and credit card data. Consumer-grade devices do not have the security features required to comply with these standards.

THE SOLUTION

Enterprise class devices are designed to provide the required levels of security, where the typical consumer class device falls short. In fact, more than half of the companies surveyed reported a security breach as a result of the use of a consumer device in the business.[2] And in BYOD programs, the majority of companies report that responsibility for security falls to the end-user — not acceptable for organizations that must comply with government regulations or face stiff penalties.[3]

Zebra Technologies goes a step beyond the typical enterprise class device security to bring healthcare organizations unparalleled security in a portfolio that provides an industry first — enterprise class devices running Android as well as typical enterprise class operating systems. While Android is evolving into an enterprise class operating system, Zebra's Mobility Extensions (Mx) adds a series of features that help make Android a more robust enterprise grade operating system, providing the peace of mind you need to deploy Zebra Android devices in your healthcare facility today.

With Android and Mx, you can prevent unauthorized users from accessing the device, as well as installing and opening unauthorized applications. Additional device controls prevent configuration errors that can take the device offline and erode worker productivity. The ability to actively detect vulnerabilities and automatically execute the right corrective action help prevent data leaks and cyber security risks.

2. Avanade survey of 600+ IT decision makers, 2011
3. Source: ITIC Survey 500 companies, July-Aug 2012; BYOD Support Points.pptx: Slide 12

"More than half of the companies surveyed reported a security breach as a result of the use of a consumer device in the business."

Source: Avanade survey of 600+ IT decision makers, 2011

SECURITY

Page 1 | Page 2

With Mx, Zebra's Android-based devices can offer the same level of security as our Windows Mobile/Windows CE devices, allowing you to confidently deploy Android in your environment. Mx is one of the many unique Zebra Mobility DNA ingredients that sets Zebra devices apart from the competition. Mobility DNA is a series of tools that boost productivity with advanced capabilities and make it easier to use, manage and develop applications for Zebra mobile devices.

Security features that our healthcare mobile device portfolio offers include:

- FIPS 140-2 government grade security rating to ensure HIPAA compliance.
- AES256 encryption for data in motion and data at rest — data is protected whether it is stored on the device, on a media card in the device or traveling over the wireless LAN.
- Remote lock and wipe for lost or stolen devices.
- Automatic locking of idle devices.
- Application permissions, which prevent users from downloading unauthorized applications that could present security weaknesses or enable uploading of sensitive data to unauthorized servers.
- Multi-user log-on, which enables a single pool of devices to serve multiple workers, yet fully control what each worker can access via log-on credentials.
- The ability to prevent automatic OS updates from the cloud, ensuring that IT has full control over determining whether an OS upgrade meets requirements for security and application compatibility — as well as if and when the upgrade should be executed.
- The ability to restrict user and application access to hardware (such as the integrated camera, GPS and Bluetooth) as well as the built-in web browser or an email client.
- The ability to remove OS features which access servers outside of the hospital network. For example, maps and email applications built into the consumer version of Android communicate with the "cloud." These connections pose a security breach risk, as personal health information (PHI) contained in healthcare applications is exposed outside of the hospital walls... and much more.

You can count on Zebra Technologies to provide the security features you need to keep sensitive healthcare data secure.

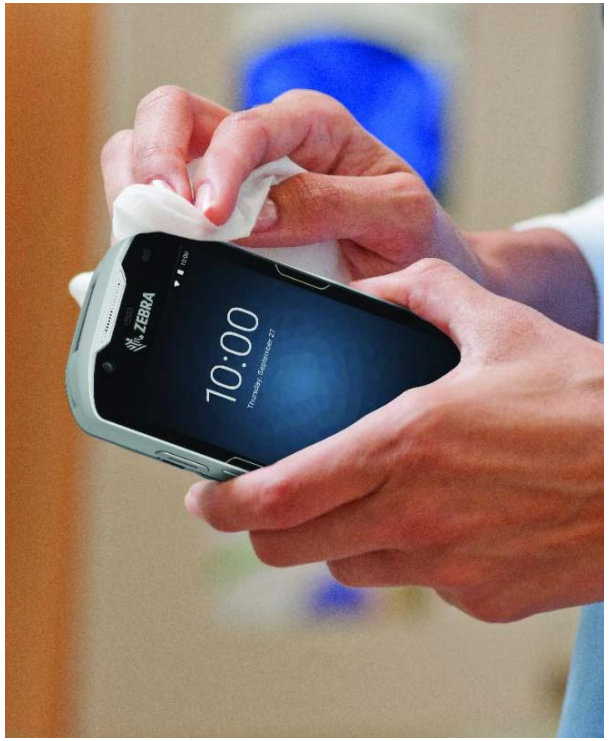
DISINFECTANT-READY

THE ISSUE

Since the mobile devices that are in the hands of your nurses and clinicians will be carried from room-to-room and patient-to-patient, you must be able to disinfect them to stop the spread of deadly infections. The risk is clear. The Centers for Disease Control and Prevention estimate that in the U.S. alone, roughly 1.7 million hospital-associated infections from all types of microorganisms, including bacteria, caused or contributed to 99,000 deaths each year.[4]

THE SOLUTION

In order to tolerate constant disinfecting in accordance with your infection control policies, the mobile device you choose will need to have the proper IP (ingress protection) sealing in order to prevent chemical cleaners from entering the device and damaging sensitive electronics, resulting in device failure. In addition, the outer plastics must also be able to withstand constant exposure to these harsh chemicals. Zebra's healthcare mobile computing devices are purpose-built with the specifications required to withstand the frequent disinfecting required to kill bacteria on contact. Alternatively, consumer grade mobile devices typically do not offer these specifications, instantly putting every patient and every healthcare worker in your facility at risk.



In the U.S. alone, 1.7 million hospital associated infections result in 99,000 deaths each year.[3] Since mobile devices are carried from room-to-room and patient-to-patient, any mobile device that cannot withstand constant disinfecting can put patients and healthcare workers at risk.

4. Pollack, Andrew, "Rising Threat of Infections Unfazed by Antibiotics" New York Times, Feb 27 2010; http://www.nytimes.com/2010/02/27/business/27germ.html?_r=0

FULL-SHIFT BATTERY POWER

THE ISSUE

The mobile device you choose must offer ample battery power for your longest shift. You don't want the devices that are providing critical patient information to run out of power at an inopportune time, nor do you want to burden healthcare workers with managing power instead of focusing on patient care.

In order to provide full-shift battery power, two things are required that consumer devices typically do not offer: a battery with the capacity to last a full shift and the ability to replace the battery. The typical consumer device battery will not last a full shift, especially since the device will be in constant use during a shift. When the battery runs low, if the batteries are not removable, the entire device must be charged. As a result:

- Productivity is reduced since workers are forced to spend time swapping devices mid-shift.
- Costs increase as hospitals are forced to either: a) purchase two devices per worker to ensure that a second charged device is always on hand if required or b) purchase sleds that contain batteries that can power the mobile device.
- Return on investment (ROI) is reduced, since devices must remain out of service for charging.

THE SOLUTION

By contrast, enterprise mobile device manufacturers recognize that continual operation is crucial, especially in the critical environment of healthcare. That's why enterprise-class mobile devices not only have high-capacity batteries capable of powering all the device features for a full shift, but also removable batteries — a fresh fully-charged battery can be inserted into a device at the start of every shift. The result? The enterprise-class mobile device remains in service all shift, every shift, providing healthcare workers with dependable access to the information they need to make split second life-saving decisions, substantially reducing the cost of mobility and maximizing the value of your mobile device investment.

In order for mobile devices to remain in service for a full shift, you need two things: a battery with the capacity to last a full shift and a removable battery than can be changed — instead of taking the device out of service for charging.

BUSINESS CLASS POWER MANAGEMENT ACCESSORIES

THE ISSUE

Consumer grade mobile devices are created for the individual and are generally single-user oriented. As such, they typically do not offer the type of accessories that will be required in the enterprise, nor do the accessories offer enterprise-class durability.

THE SOLUTION

Enterprise class devices offer purpose built accessories that simplify and reduce the cost of backroom management. For example, consumer class devices generally require one charger per device, and each charger requires its own outlet. By contrast, enterprise-class devices offer multi-slot chargers that allow you to use one outlet to typically charge at least four devices or four batteries simultaneously. As a result, the enterprise class device requires only a quarter of the outlets that consumer devices will require. And since a multi-slot charger commonly takes up less space than four individual chargers, you'll need less space to support each shift.

In addition, unlike consumer accessories, enterprise accessories are built to business grade specifications, such as the number of insertions a cradle can handle before contacts wear out. By contrast, consumer charging accessories — including sleds — typically do not offer an insertion rating.

Without enterprise-grade accessories, if you choose company-owned consumer class mobile devices, backroom infrastructure costs can soar. Without industrial design, all day around-the-clock use may wear out the accessories before the device. In addition, you may need to purchase new cradles and chargers every year as consumer device models change, which may also trigger the need to modify the back room design.

Enterprise-grade accessories are designed to last longer, perform better and save space. Over the long term, they also are more cost effective.

ENTERPRISE SCANNING PERFORMANCE

If the mobile device you choose lacks industrial class barcode scanning, the result can be a major impact on the productivity of your healthcare workforce.

THE ISSUE

In your hospital or clinic, one of the most important features of any mobile device you put in the hands of your nurses and clinicians will be barcode scanning. It is barcode scanning that will positively identify patients, medication, specimens and more, preventing errors that can result in illness or death. And it is barcode scanning that will allow you to seamlessly implement healthcare Barcode Medication Administration (BCMA) requirements.

THE SOLUTION

Enterprise mobile devices offer integrated high performance barcode scanning that is in a completely separate class from the scanning capabilities of consumer class devices. For example, Zebra's healthcare mobile devices offer dedicated scan engines that can capture virtually any barcode in any condition — 1D or 2D, regardless of whether it is damaged, scratched, dirty or poorly printed. In tests performed by Scandit, Zebra's scan engine captures barcodes 20 to 50 times faster than consumer mobile devices. And where consumer devices returned an erroneous barcode read as much as 10 percent of the time, the Zebra scan engine mis-decode rate was negligible, at just 0.005 percent.[5]

A lack of industrial class barcode scanning can have a major impact on the productivity of your healthcare workforce — though this drain is often well-hidden and unaccounted for in TCO analyses. For example, slow read times can turn into hours of wasted time and frustrated workers. Let's take a look at the math.

THE NUMBERS

On average, a nurse scans 20 barcodes per hour over an 8 hour shift. Using consumer technology, each scan takes two seconds for a total of 5.3 minutes per shift. When you extend that time to the nursing staff of a small hospital with 32 nurses per shift (96 shifts per day), nearly eight and half hours — the equivalent of one full nurse shift — are spent just scanning barcodes each day. Using enterprise technology developed specifically for hospital use, that time is only about 25 minutes. Over the period of a year, using enterprise technology instead of consumer can translate into a time savings of 2,939.5 hours, the equivalent of adding 1.4 nurses to your staff, greatly improving productivity.

5. Scandit Scanning Performance: http://www.scandit.com/barcode-scanner-sdk/features/performance/

SCANNING PERFORMANCE

Feature	Scanning Application on Consumer Device	Zebra Scanning Technology (SE4500)
Omni-directional	Often < 30 degrees[1]	360 degrees[2]
Decode Time	2-5 seconds[4]	Typical < 100ms[2,3]
No Read	Up to 30%[4]	Typical < 1%[2,3]
Mis-decode rate on UPC A	Up to 10%[4]	Typical < 0.005%[2,3]

1 – Zebra Technologies test 2– Zebra Technologies specification 3 – Typical performance 4 – Scandit

SCANNING SPEED: IMPACT ON NURSE PRODUCTIVITY

ENTERPRISE VS. CONSUMER GRADE SCANNING TECHNOLOGY		
Scan Time	**Consumer Technology**	**Zebra Enterprise Technology (SE4500)**
Time per scan	2 seconds	100 ms
Scan time per nurse shift (Assumption: 20 scans per hour)	5.3 minutes	16 seconds
Daily scan time per hospital (Assumption: 96 total nursing shifts)	8.48 hours	25.6 minutes
Annual scan time per hospital	3,095.2 hours	155.73 hours

Numbers based on a small hospital with 32 nurses per shift, 96 shifts per day.

Over the period of a year, the time saved through enterprise scanning performance can translate into the equivalent of adding 1.4 nurses to your staff.

SCANNING APPROACH: NATIVE INTEGRATED VS. AFTER MARKET "SLED" ATTACHMENTS

THE ISSUE

Consumer mobile devices do not offer integrated industrial barcode scanning — the one feature that nurses, physicians, pharmacists and lab technicians consistently use to identify patients, access patient information and protect against errors that can threaten patient health. While enterprise devices offer built-in native scanning, the only way to add scanning to a consumer device would be by adding a "sled" — an accessory that typically encases the phone.

There are numerous potential pitfalls related to sled attachments you'll need to examine:

- **Compromised Wi-Fi performance.** The electronics in the sled can interfere with the antenna, and the sled itself might block the area where the antenna is located. As a result, the consumer mobile Wi-Fi antenna can be negatively impacted, degrading wireless performance, impeding critical staff communications and potentially affecting patient care quality.
- **Lack of sealing.** Consumer sleds typically lack sealing, which is intended to improve durability and provide protection against liquids entering the device. Without the sealing found in enterprise devices, chemical cleaners can corrode fasteners, USB connections and electrical contacts, adversely affecting device performance. Additionally, lack of sealing between the consumer device and the sled creates a gap where bacteria can enter and bodily fluids can pool, turning a tool meant to improve patient care into a vehicle that can unintentionally increase the spread of infections.
- **Reduced ergonomics.** The ergonomics of the consumer mobile device are changed when a sled is added, impacting size and balance. This cumbersome configuration can negatively affect user experience and the efficient delivery of patient care.
- **Higher device costs.** Sleds can significantly increase your device acquisition costs due to:
  - High initial costs. Utilizing a sled increases upfront consumer mobile device costs by as much as 50%.
  - High replacement costs. Since sleds are typically designed for a specific model and are often not compatible with the next generation device, you will most likely need to purchase a new sled when you purchase a replacement consumer device.

THE SOLUTION

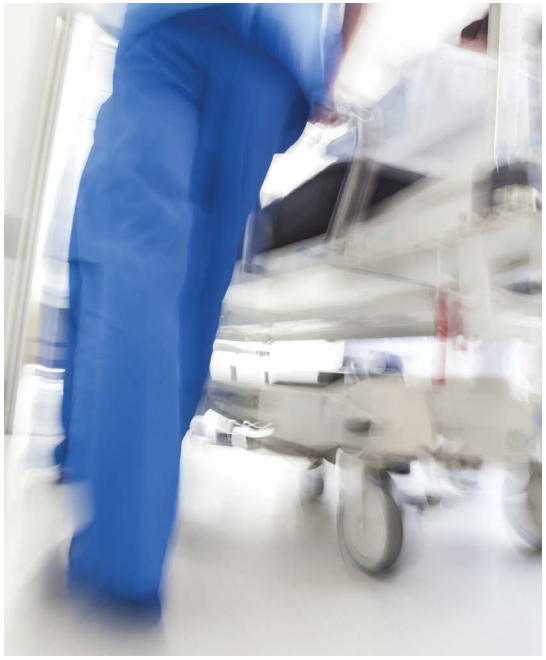
The issues associated with adding a consumer device sled for scanning can be eliminated by choosing enterprise-class mobile devices designed for healthcare with integrated industrial barcode scanning as a base feature.

Sleds can impact mobile device ergonomics and economics — sleds often cost two to three times that of the consumer mobile device, making total acquisition cost on par with the typical enterprise class device.

DURABILITY

THE ISSUE

Inevitably, the mobile device your healthcare workers use will be subjected to drops and spills — the device you choose should continue to operate reliably within these conditions. As a result, durability should be a key criteria — without it, devices will require frequent repair and replacement.



THE SOLUTION

The device you choose should offer specifications that ensure the level of durability you require, such as:

- **A drop specification:** The drop test ensures that the device can handle a free-fall from a specific height to a specific type of floor (such as tile or concrete).
- **A tumble specification:** Where the drop test ensures that a device can handle the impact of a single hit, the tumble specification ensures that the device can endure the multiple hits that occur when a dropped device tumbles before coming to a rest.
- **Ingress Protection (IP) sealing:** A worldwide standard, IP sealing ratings ensure reliable operation, even when exposed to a liquid spill and dust. Ratings vary from the ability to handle water drops, splashing and even complete immersion in water, as well as dust-resistant to completely dust-proof.

Consumer devices rarely offer these specifications — as a result, they are much more fragile than their enterprise counterparts, which typically offer these specifications to ensure that the device can provide the lifecycle and the enterprise TCO your organization requires.

The numbers are in — the cost of just one or two instances of device failure can easily justify the additional cost of a rugged device.

THE PROOF

A recent study by VDC Research Group[6] validates the value of choosing an enterprise-class device over a consumer device. Consumer devices are three times more likely to fail in the first year. The average first year failure rate for rugged devices is 7 percent, compared with the 23 percent for consumer devices – and consumer device failure rates in excess of 50 percent are not uncommon. The cause of 77 percent of those failures is a dropped device, which resulted most commonly in a cracked display. The cost of all those failures is high — not only does the device require repair or replacement, but every failure can result in 180 to 260 minutes in lost mobile worker productivity and additional internal support. The cost of just one or two instances of device failure can easily justify the additional cost of a rugged device.

6. Mobile Device TCO Models for Line of Business Solutions; Volume 1/Track 7: Enterprise Mobility Mobile Device TCO; David Krebs; VDC Research Group, Inc.; 2012 (Slides 4, 18, 28 and 29)

MANAGEABILITY

THE ISSUE

Centralized management is a must-have for mobile devices. Without it, IT must physically touch a device for everything from preparation for use to troubleshooting and resolving device issues.

Consumer grade devices are not easily supported by industry-standard enterprise-class mobile device management (MDM) solutions, often translating into very expensive support costs. And those costs can rise substantially with BYOD initiatives. Since your IT department is unable to monitor and troubleshoot BYODs from an MDM application, you have two choices.

1. Your employees can bring devices to your IT help desk, which means help desk personnel will be responsible for learning about potentially hundreds of models — models that change every 12 to 18 months.

2. More likely is the alternative scenario — your employees become responsible for figuring out where to get support, resulting in the loss in productivity, as well as the fact that you have lost control of the support process.

THE SOLUTION

Alternatively, today's enterprise class mobile devices do support centralized Mobile Device Management (MDM) solutions, which can enable IT to remotely stage, update, monitor, troubleshoot and lock and wipe devices, no matter where they may be. In addition, IT can receive alerts and alarms that signal the start of a device issue before the user is impacted, enabling the proactive response that can eliminate device downtime and the resulting impact on user productivity. IT can better manage your mobile devices, with very little dedicated time required.

Zebra Technologies takes mobile device management a step further to include our enterprise class Mx Android-based devices. While the standard version of Android does not support MDM, our Mx Android supports enterprise-class management. As a result, your IT department can manage all Zebra healthcare mobile devices from a single pane of glass, bringing enterprise-class management to a consumer grade operating system.

According to VDC Research, the result can be a significant reduction in support costs:

"Effective use of device management solutions — for remote diagnostics, software upgrades, etc. — can reduce the average annual support costs per mobile worker by as much as 85%." [7]

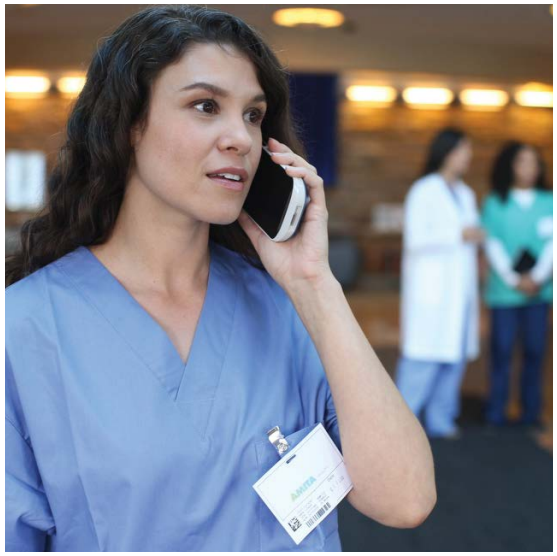
Selecting effective device management solutions can reduce average annual support costs per mobile worker by as much as 85%.[7]

7. VDC Research, White Paper — Enterprise Digital Assistant Leverage in the Emerging Mobile Enterprise; David Krebs/Chris Rezendes; Jan 2010

VOICE COMMUNICATIONS FLEXIBILITY

THE ISSUE

When it comes to enabling your workers, mobile voice is just as important as data. Without it, you may need to provide workers with more than one device to enable different types of voice capabilities. For example, nurses may need to make an instant push-to-talk call in an emergency to other co-workers in the building or take a call coming through the PBX from a patient's family member.



THE SOLUTION

To create the true all-in-one voice and data mobile device, we developed Zebra's Enterprise Voice Solution. Unique in the industry, this solution allows you to easily add the voice features different workgroups need on our mobile devices. And since all services are delivered over the Wi-Fi network, there are never any monthly cellular fees. In addition, with our Validated Voice Solution, you can be assured that the voice services you deploy will work on the technologies you have — including mobile devices, wireless LAN infrastructure and PBXs.

Key voice features. With our complimentary Push-to-Talk Express client software (pre-installed on most Zebra devices), you can enable push-to-talk (PTT) between Zebra devices, right out of the box. In addition, you can turn our mobile computers into desk phones, complete with an extension number and PBX time-saving features such as call forwarding and 3-way calling. The result? You can eliminate the cost of separate desk phones and simplify life for your workers, who no longer need two separate devices for voice and data. And you can get more value out of your existing PBX.

In healthcare, mobile voice is just as crucial as mobile data — your staff needs to be reachable in an instant. Enterprise mobile devices can support everything from instant push-to-talk to the ability to double as a mobile desk phone — maximizing your mobile device investment and reducing the need to carry multiple devices.

LIFECYCLE MANAGEMENT

THE ISSUE

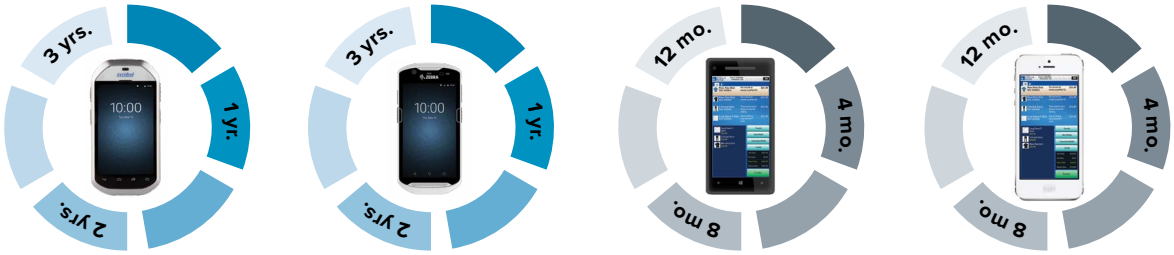
The rate of device churn — when new devices are released and their older versions are retired — is another item that should be high on the criteria list, yet is often overlooked. The reason this criteria is crucial is the hidden costs of fast churn.

In the world of consumer mobile devices, one year is typically the maximum time a specific model is available, with no guarantees that the next model provides backwards compatibility for accessories and applications.

THE SOLUTION

In contrast, for enterprise mobile device manufacturers, device churn is measured in years instead of months. For example, Zebra's healthcare mobile devices are not only built to last for a minimum of three years, they are also guaranteed to be available for purchase for a minimum of three years, with an additional three years of support once the device has been discontinued. Since enterprise mobile device manufacturers are focused on business instead of consumer needs, when a next generation device is released, you can typically count on a smoother and more efficient backward compatibility process. This strategy allows you to more easily implement next generation technology and helps minimize resource-consuming transition processes.

Enterprise class device lifecycle is measured in years...and consumer class device lifecycle is measured in months.



When you choose an enterprise class mobile device, unlike consumer grade mobile devices, there is typically no need to purchase new accessories, further reducing capital costs and TCO. And if the device you choose has a platform strategy, like Zebra Technologies, entire portfolio of healthcare mobile computers, applications can typically be ported to the new devices with little or no development effort, reducing operational costs.

Consumer mobile devices are typically available for purchase for only one year. As a result, when you add new workers or need to replace broken devices, you can end up with many different models to support, each with their own unique accessories — driving up capital and operational costs.

SUPPORT SERVICES

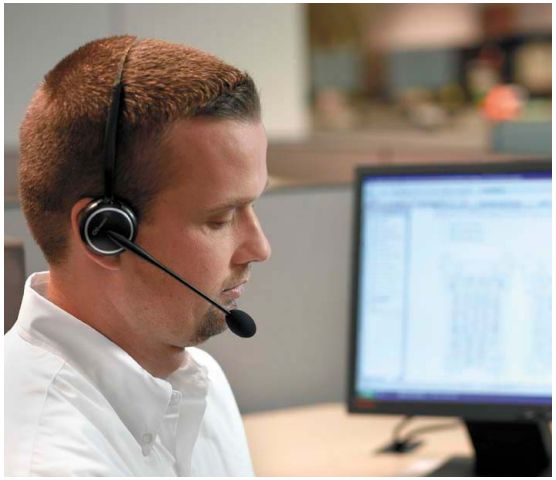
THE ISSUE

What happens when a device needs repair? Can you get the same level of service for enterprise and consumer mobile devices?

With consumer grade mobile device support services, workers may be without a device for days. And when the device is returned, the worker will need to restore all the data. The result is a level of device downtime that degrades TCO and worker productivity. Yet there is no real alternative: since there are so many different types of consumer models and they change regularly, keeping a spares pool on hand isn't feasible.

THE SOLUTION

Enterprise mobile device manufacturers understand that device downtime is not an option — and that fact is reflected in their support programs. For example, Zebra Technologies offers optional cost-effective business-grade support programs that include everything from normal wear and tear to accidental breakage — including a broken screen on a device that was dropped. No matter what the problem is or what caused it, it's covered. In addition, our overnight replacement option provides a mobile device that has already been provisioned with your software applications and device settings, so workers are back up and running the moment the device is removed from the box.



Device downtime is not acceptable in the mission-critical environment of healthcare. You need to keep your devices up, running and in the hands of your healthcare workers. That requires a support plan that will cover everything and offer overnight replacement of broken devices — a level of service you won't find for the typical consumer smartphone.

The math.

The truth is in the numbers — consumer class devices come at a high cost.

The numbers are in. They reveal that while, at first glance, it may appear that lower cost consumer-grade mobile devices and BYOD programs that allow workers to use their own consumer-grade mobile devices are the way to the most cost effective and most successful healthcare mobility solution, the numbers show otherwise — and numbers never lie. Consider the following facts:

CONSUMER CLASS DEVICE TCO IS SUBSTANTIALLY HIGHER.

Consumer grade devices cost an average of 50% more over a 5-year period: the annual five-year TCO for a small consumer grade device is more than 50% higher than its enterprise grade counterparts. The annual five-year TCO of an enterprise grade device is $2,140, while the consumer grade device costs $3,236 over the same time period.[8]

CONSUMER CLASS DEVICE ACQUISITION COSTS ARE THE SAME — OR HIGHER.

In order to develop an "apples-to-apples" comparison of consumer vs. enterprise class hardware costs, you'll need to factor in lifecycles: enterprise class devices are built to last three to five years, while consumer device life expectancy is just one to two years. So while that consumer grade mobile device appears to be less expensive, be sure to factor in that over the course of the lifecycle of one enterprise class mobile computer, you'll likely need to purchase two to three consumer mobile devices and two to three sleds. The result? Hardware acquisition costs over a three to five year period for enterprise class are ultimately less than consumer grade mobile devices.

For example, based on the list prices of some of today's most popular products, a sled is approximately $300 and a consumer-style data mobile device is roughly $600. In order to serve your hospital for three years, you would need to purchase a minimum of two sleds and two consumer style devices, for a total hardware cost of $1,800. For that same time period, only one enterprise class device would need to be purchased at a cost of $1,500, making the selection of the consumer-style device cost 20 percent more.

33% THE AMOUNT THAT CONSUMER CLASS BYOD CAN INCREASE YOUR SUPPORT COSTS

Aberdeen Group reported that a company with 1,000 mobile devices can expect to spend an average of an extra $170,000 per year to support BYOD. The following five well-hidden costs can result in a 33% increase in operational costs for BYOD initiatives:[9]

1. Carrier billing is no longer aggregated, which can result in missed discount opportunities and larger monthly fees
2. Increase in IT time to manage and secure corporate data on employee devices
3. Increase in support costs due to the increase in types of mobile devices and their durability levels
4. Increase in the workload for other operational groups that are not normally impacted by mobility support
5. Increase in the number of expense reports filed by employees for reimbursement of device-related expenses

8. Mobile Device TCO Models for Line of Business Solutions; Volume 1/Track 7: Enterprise Mobile Device TCO; VDC Research Group, Inc.; Mobile and Wireless Practice; February 2013
9. BYOD: If you think you're saving money, think again; Tom Kaneshige; April 4, 2012; CIO; http://www.cio.com/article/2397529/consumer-technology/byod--if-you-think-you-re-saving-money--think-again.html

Seven steps to a successful mobility deployment.

Clinical mobility is transforming the ways hospital staff communicate and collaborate and is having a profound impact on improving the quality of patient care. A well-thought-out implementation plan is essential for taking your vision off the drawing board and into the real world. The path to a successful mobility deployment begins by following these seven critical steps.

1. Share insights and information.

During the mobility strategy phase of your implementation, you identified key user groups and interviewed stakeholders. Now it's time to convene a cross-functional project team — including representatives from clinical staff, IT, security and facilities — so that they can share insights and information about their specific requirements and align them with the hospital's strategic business requirements.

Project team members should assess the clinical environment by actually walking the hospital floors, reviewing department floor plans and evaluating specific workflow considerations. By sharing information, your team will be able to develop a project plan that satisfies criteria at every level — from your health IT department to critical care nurses working in the ICU.

2. Conduct a site assessment.

Having defined the day-to-day needs of end users, the next step is to assess your hospital's infrastructure and its ability to support the new mobile deployment. This assessment should include a review of the facility's physical environment and take into account the building's construction. Many older buildings were built with very dense construction materials that can slow network speeds or even completely block wireless signals. This can have a detrimental effect on mobile applications that are extremely sensitive to even the slightest drops in connectivity.

To make certain that your mobile devices operate when and where they are needed, it is vital to test the strength and reliability of the wireless infrastructure throughout your facility — everywhere mobile devices roam even down to the patient bedside. By doing so, you will ensure that the system provides adequate reliability, performance and coverage to support your mobile data and voice requirements.

Then, identify all devices that will be deployed in each hospital unit – including workstations on wheels and patient monitoring devices in patient care areas as well as administrative, housekeeping and other auxiliary locations.

Finally, the IT department will want to carefully evaluate the systems integration requirements for the hospital's legacy systems, biomedical devices and the electronic health record (EHR) system to support data-driven closed-loop communications.

You might want to consider bringing in a third-party advisor to assess your wireless infrastructure in terms of its ability to support applications and devices and to assess how your EHR system may influence your deployment.

3. Build security into your plan.

Protecting patient health information must be a high priority for all healthcare organizations and IT departments must ensure that their institutions are compliant with HIPAA and the HITECH ACT regulations. Safeguards must be put in place to address potential risks and prevent unauthorized access. Oftentimes, IT departments make use of multiple levels of security to prevent unauthorized access to data such as device encryption, SD card encryption and complex passcodes.

Centralized controls and built-in security features are also essential to enable you to remotely wipe data and track the location of a device in the event it is lost or stolen, as well as to block or remove unauthorized applications. Be sure to make use of mobile device management tools to protect patient data and enable visibility and control of all devices without affecting staff performance and patient care.

4. Map the implementation process.

Your mobility strategy should include a comprehensive rollout plan. Many healthcare institutions find that a multi-phased approach is less disruptive to their operations and easier to manage for both staff and administration. In mapping the implementation process, be sure to include clear definitions of all procedures and processes required for effective deployment of your new mobile devices. Finally include a course of action for a well-planned and well-documented in-house training program.

How a pocket-sized mobile device helped reduce patient falls by 40%

The central nursing stations at a 240-bed acute care hospital were not integrated with bed exit alarms, making nurses solely dependent on audible notifications. The lack of integration was exacerbated by the geographical layout of the units, which includes long hallways, making it difficult to hear an audible alarm sounding in a patient's room.

The hospital collaborated with Extension Healthcare, an alarm management and event response platform, to integrate the hospital's clinical system with the Engage Mobile application and Zebra's mobile computing device. The Engage system color-codes alarms based on their urgency and automatically flags those that require immediate attention. In the first two years alone, the hospital reduced falls by 40% and achieved an ROI of $1.06 million — a significant quality process improvement.

5. Establish clinical mobility policies and training programs.

You'll need to develop and publish a facility-wide policy that identifies appropriate end-user usage models for hospital and personally owned mobile devices. Hospital leadership should strongly encourage, if not mandate, that all clinical communications leverage the organization's smartphone-based enterprise communications platform. The IT team should provide guidance about how hospital-owned mobile devices will be stored, tracked, managed and recharged.

Human resources and individual medical departments may want to conduct regular new-hire and in-service training sessions to educate care providers and other mobile hospital workers on how best to use mobile devices to enhance communications and patient care.

6. Establish a support/help system.

Planning ahead for any potential issues or problems is a critical step before rollout. Your hospital IT team may need to retrain or hire additional help desk personnel with the appropriate skills, knowledge and expertise to help end users:

- Troubleshoot mobile device and system interoperability issues
- Answer application questions
- Resolve connectivity issues and escalate when required

Be sure to have a contingency plan in place to ensure the availability of backup devices and batteries when and where they're needed. Confirm that you have a service agreement in place with your technology and solution partners. Keep documentation about new policies and procedures on file for future reference.

7. Institute a user-feedback loop.

In the weeks and months after deployment, closely monitor end-user feedback through the use of surveys, usage reports, direct observation and hospital IT service desk tickets. Encourage end users to suggest new and innovative ways that mobile device-based communications can be used to improve team-based collaboration.

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
+1 866 230 9494
la.contactme@zebra.com