White Paper

Enterprise Mobility Management: To Improve Clinician Workflows and Patient Outcomes, Think Beyond the Device

Enable better care with a solution that harnesses the full potential of mobile devices and apps.

Modern healthcare is being transformed by the incredibly fast adoption of mobile devices, new mobile health (mHealth) apps, the consumerization of IT, and rising expectations for bring-your-own-device (BYOD) and flex-work policies, especially among younger clinicians. While these trends promise powerful benefits for today's healthcare providers, they often pose significant challenges for IT.

First, let's look at the opportunities. Mobile devices and apps can transform healthcare by:

- Putting information at clinicians' fingertips for faster decision-making at the point of care.
- Enabling better communication and coordination among caregivers and staff (many of whom work 12-hour shifts or are not always on call) and directly with patients.
- Integrating innovative and exciting mobile technology into recruiting and retention strategies.

The opportunities provided by mobility make it possible to increase business agility, productivity, and job satisfaction by permitting healthcare professionals to use innovative new mobile apps. Delivering care anywhere, anytime makes healthcare more efficient, and therefore, more cost-effective in providing better patient outcomes.

The challenge of mobility for IT

To enable this flexibility, IT must be able to secure apps and data on a potentially unlimited variety of mobile devices, over any kind of network, in any location – even when the same devices might contain personal apps and data. The challenge is to balance clinician or staff workflow needs, desires, and preferences with the complexity and potential security risks of mobility to ensure that the power of these devices and apps can be harnessed for healthcare.

Specific challenges include:

- Supporting and managing the sheer number of devices being used in healthcare (A recent Epocrates study found that 41% of clinicians use three devices: tablet, smartphone, and computer. That's projected to jump to 74% by the second quarter of 2015[1]).
- Handling the complexity associated with supporting and managing heterogeneous device operating systems.
- Supporting personal or BYO mobile devices in the right way.
- Introducing new native mobile apps (for example, clinical, productivity, or business apps) alongside Microsoft® Windows® and web applications to turn mobile devices into valuable tools for clinicians and staff.
- Addressing diverse users (for example, clinician vs. administrative staff, employee vs. affiliate) and access scenarios (for example, in a hospital on a corporate wireless network or on a guest patient network).

Trying mobile device management

To address these challenges, many IT departments attempt to implement solutions that manage the mobile devices themselves. Mobile device management (MDM) solutions

[1] Epocrates Inc., an athenahealth Inc. company, "Mobile Trends Report," 2014

can be highly effective for protecting sensitive patient and business information, controlling the mobile apps that can be used, remotely wiping lost or stolen devices, and other essential functions.

Although MDM is vital, it should be considered only the first step in gaining control over, and fully exploiting the capabilities of, mobility in healthcare. While suitable for many types of workers in static environments, many MDM solutions were not built with the flexibility to address healthcare's diverse use cases that are based on individual requirements for security, compliance, and mobile functionality.

A more comprehensive solution has to go further in managing three key aspects of mobility: device proliferation, support for native apps, and diverse user scenarios. Organizations are now adopting a new approach in which MDM is only one component of a more comprehensive set of capabilities through which IT can manage the devices plus their apps and data. Known as enterprise mobility management (EMM), this approach is playing an increasingly central role in the new era of IT.

Device proliferation and diversity

The consumerization of IT, in which the individual adoption of advanced mobile devices often outpaces corporate adoption, has blurred the lines between work and personal life. Healthcare executives and clinicians typically buy smartphones and tablets for personal use and see no reason why they shouldn't be able to use them for work as well. Increasingly, caregiving is perceived as something you do, not a place you go to, and it can happen anywhere at any time.

The focus is on productivity, not on the abstract notions of ownership, preferred devices, or IT standards. Indeed, the Epocrates 2014 Mobile Trends Report characterized almost half of their survey respondents as "digital omnivores," clinicians who use a tablet, smartphone, and laptop or desktop computer routinely to do their jobs.[2] Without IT playing its customary role in enforcing standardization, the mobile devices flooding healthcare environments come in all varieties: not just Apple® iOS® and Google® Android® but also proprietary third-party Android and Microsoft Windows platforms.

This challenge will get exponentially greater as graduates of top medical schools enter the workforce. Recent graduates have grown comfortable using these devices in multiple settings, and the distance between personal use and recognizing the potential for getting work done is negligible. This isn't a bad thing; healthcare systems should want their clinicians thinking about ways to be more productive.

In addition, the pressures placed on healthcare to deliver better outcomes at lower cost demand the adoption of innovative mobile apps to increase clinician productivity. Therefore, IT's mission is more and more about empowering people with the tools that will help them improve care. But this requires thinking through all of the diverse mobile devices, app types, and user or access scenarios that may be coming.

Native mobile app support

Consumer apps have quickly moved into the enterprise, flooding the market with thousands of new mHealth apps. Furthermore, providers are developing mobile apps in-house to immediately improve care delivery and business decision-making. These range from productivity apps such as secure mobile email, secure texting, and secure note-taking to purpose-built clinical applications.

[2] Epocrates Inc., an athenahealth Inc. company, "Mobile Trends Report," 2014

RxPhoto is a great example. Developed by AppwoRx, this Citrix Worx-enabled app is a photographic record keeping platform that dramatically improves the efficiency and accessibility of clinical photography. It revolutionizes the way medical photography is integrated into the practice of medicine through:

- **Anatomy cataloging** that provides 3D image selection, permitting you to catalog over 300 anatomy areas.
- **EMR integration** that integrates photos and patient data directly into the individual's electronic medical record (EMR).
- **Photo ghosting**, which uses the previous photo as a guide for new photos to help users take consistent images.
- **Mobile gallery** that allows you to view and manage existing photos.
- **HIPAA-compliant cloud storage**, which saves images without ever storing them on the device.

Diverse users and access scenarios

As noted, modern IT departments are challenged to secure and control the full diversity of mobile devices and apps given the unique requirements, security risks, and access scenarios that must be supported for distinct user groups. Healthcare providers must take into account a user's job role, clinical specialty, and employment terms when thinking about the level of flexibility offered with mobile devices and mobile apps. They must also consider whether the same level of access to apps and data should be granted as people work across different locations.

For example, while a group of visiting nurses and mobile clinicians that practices in a variety of facilities benefits from mobility, both their requirements and the security parameters set in each environment may be very different. Roaming clinicians need a certain set of applications while visiting nurses use another. Another critical consideration is whether they're affiliates or employees. What networks are they using to gain access? And what tools should or shouldn't be available depending on those access scenarios? Would you give a nurse the same level of access to apps with protected health information (PHI) both inside and outside the hospital? Or, would you want to grant access to communication tools inside and outside the hospital but not to an EMR app (such as EpicCare's Haiku and Canto).

A multipart solution: enterprise mobility management

From a provider and IT perspective, the key is to own a complete EMM solution with comprehensive, granular capabilities to secure and control the devices themselves as well as the apps and data they contain for unique users. That's exactly what Citrix® XenMobile® does. The solution:

- Gives users device and app choice while ensuring compliance.
- Delivers business-class productivity apps that users love and IT embraces.
- Enables business by allowing simple, scalable, and anywhere access to apps.
- Provides advanced app and data controls to keep users happy while assuring content security for IT.

Mobile device management: A first step toward securing mobile devices

For healthcare organizations seeking control over the mobile devices in their environment and the way they are used, MDM can be an important step. Citrix XenMobile includes enterprise-class MDM capabilities, which provide role-based management, configuration, and security for hospital- and employee-owned devices throughout the device lifecycle. IT can enroll and manage any device, detect "jailbroken" devices, and perform a full or selective wipe of a device that is out of compliance, lost, stolen, or belongs to a former employee.

Application security is ensured through secure application access via app tunnels, blacklisting and whitelisting, and dynamic, context-aware policies. Network security capabilities provide visibility into and protection against internal and external mobile threats; blocking of rogue devices, unauthorized users, and noncompliant apps; and integration with security information and event management (SIEM) systems. As a result, IT can provide people with the freedom to choose the devices they want to use while ensuring compliance requirements are met and business information on the device is secured.

Mobile app management: Embracing BYOD and any mHealth or business app

As effective as MDM can be, it is only one component of a complete mobile strategy. As progressive healthcare providers become more open to BYOD practices, they need to assess how they will secure personal devices used in the clinical setting.

In addition, many mobile apps introduce unacceptable security gaps, such as those that move or store data via third-party clouds. Simply blacklisting these apps for all users would limit the capabilities available to the healthcare system. A better approach would be to focus on controlling the way the data within these apps is secured, stored, and used, enabling IT to allow them for select use cases.

The mobile application management (MAM) capabilities in Citrix XenMobile enable complete management, security, and control over native mobile apps and their associated data through several advanced techniques.

Separating business and personal apps and data in a secure mobile container

With the Citrix MDX app container technology, IT creates a secure container around healthcare apps and data to isolate that content from personal content on a user's mobile device. This container enables full control over all the content via automated usage policies and direct administrative actions, while delivering a rich, native user experience. IT can secure any custom-developed, third-party, or BYO mobile app with comprehensive policy-based controls, including mobile data loss protection (DLP) and the ability to remote lock, wipe, and encrypt apps and data.

Enabling seamless interaction between containerized business apps

With the Citrix MDX inter-app controls, IT determines how containerized apps interact with each other. They can block nonprotected or personal apps from interacting with containerized apps. IT can also enforce rules governing specific inter-app policies, for example, deciding to allow cut-and-paste between containerized apps, but not to unprotected or managed apps. Or they can ensure that every hyperlink clicked in their secure, business email app automatically opens in a secure mobile browser rather than a default browser such as Safari.

Providing granular, policy-based controls and management over all HTML5 and native mobile apps

The MDX Access technology enables IT to centrally control and configure policies specific to each mobile app. For example, IT can set policies around the type of devices or network required for app access. MDX Access also provides the industry's first application-specific micro virtual private network (VPN) for accessing a hospital's internal network, preventing the need for a device-wide VPN that can compromise security. The app-level VPN also improves the user experience by eliminating additional credentials when off a corporate-owned network; for example, clinicians could access a hospital or patient portal without entering their credentials over a guest wireless network such as those unprotected for patient and visitor use.

Healthcare-ready mobile productivity apps and data management: a quick win with clinicians, executives, and staff

What's the benefit of a mobile device like a smartphone or tablet if your clinicians or healthcare executives can't use it to securely communicate with other caregivers, staff, or patients, or access and send the medical or business data they need to be productive? That's why many providers want enterprise-ready mobile productivity apps as their quick win with powerful mobile users like executives and doctors.

XenMobile includes a robust suite of Citrix-developed, business-class mobile apps that are fully containerized on the mobile device, separate from personal apps, to ensure secure productivity:

- **WorxMail™** – a containerized email, calendar, and contact app with a rich user experience that helps coordinate clinician activities as part of a unified healthcare team
- **WorxWeb™** – a consumer-like browser that provides access to Internet and intranet sites and is secured according to IT policy. This provides medical researchers or clinicians who just want to stay current with access to these resources but in a secure manner.
- **ShareFile®** – an app that allows mobile users to share, sync, and edit files to help keep patient records up-to-date as they move through the system from admissions to examination to discharge. ShareFile provides a brilliant and intuitive experience on mobile devices as well a mobile-optimized website as an alternative way to access and securely share data.
- **WorxNotes™** – a business-class secure note-taking application with email and calendar integration for streamlined mobile workflows. Clinicians can securely create, sync, and share notes about a patient, for example, with specific user groups using WorxNotes with "one-click" distribution and Microsoft Outlook integration. Search and store notes simply through WorxNotes integration with ShareFile.
- **WorxDesktop™** – a secure remote access app that allows healthcare providers to access their desktops from a mobile device. They can instantly open any desktop software in full-screen mode (MphRX, MyAppWorx, TigerText, etc.), and access files and apps from any computer. Hospital intranets and internal resources are accessed through a VPN tunnel.
- **WorxEdit™** – an easy-to-use editing tool for mobile devices, allowing clinicians to edit documents, spreadsheets, and presentations. Clinicians can open, view, create, and edit Microsoft Word®, Excel®, and PowerPoint® files, and collaborate with others using track-change capability.
- **GoToAssist™** – an app that simplifies support with instant "one-touch" help-desk access for mobile users who can open service desk tickets or request live support directly from their devices to avoid any interruption in providing patient care.

Workflow-driven mobile productivity

The best-of-breed apps described previously go a long way to improving mobile user productivity in healthcare. But they can do more when used together to increase productivity in workflows.

A workflow typically consists of several tasks and steps that must be completed efficiently. And rarely will a mobile user be able to accomplish a workflow using a single application.

But taking a workflow-driven approach to mobility can help achieve productivity gains that come with a family of productivity apps delivered from a single vendor. These apps are built to work together in an effort to streamline mobile workflows by reducing the number of steps it takes to complete complex workflows. Let's look at a couple of examples.

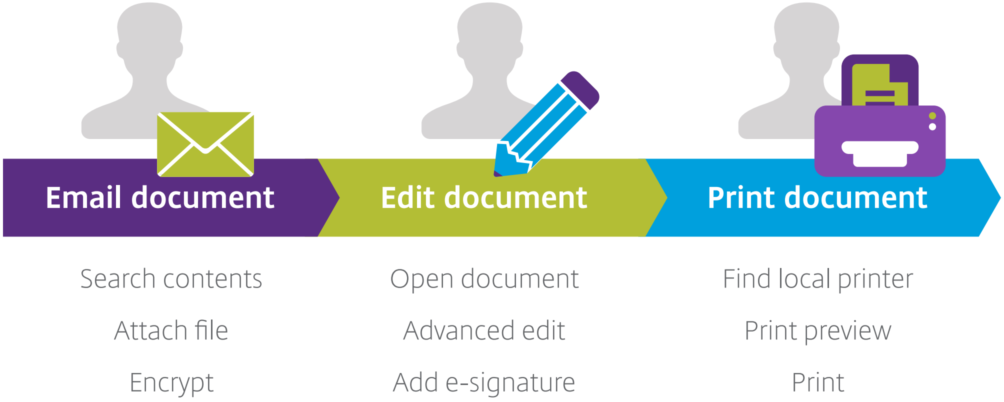

Figure 1. Sample workflow streamlined by XenMobile

Sample workflow: signing and printing documents

Figure 1 depicts a common workflow that can be streamlined with the XenMobile solution.

Although healthcare is well into the digital age, not everything is paperless yet, and it still requires hardcopy signed documents. In this example, the integration between WorxMail and ShareFile creates an unmatched user experience for the mobile user working with a combination of softcopy and hardcopy documents.

The user receives an encrypted message and document in their WorxMail inbox. From WorxMail they can open the document and launch right into ShareFile with no additional passwords or credentials. ShareFile's advanced editing capabilities allow the document to be edited and modified.

ShareFile also has the ability to add your unique signature to the document. The signature feature can be used for both Microsoft Office and Adobe Acrobat (PDF) documents and can be sized, moved, and placed exactly where you need it. Once the document has been signed, it can be sent to a local printer without launching any additional applications.

Sample workflow: "follow-me data and apps"

Clinicians often have fragmented work schedules, moving from meeting to meeting, patient to patient, and venue to venue. But we can boost their productivity when on the move by allowing them to securely connect to their physical desktop (or laptop) for "follow-me data and apps."

In this scenario (see figure 2), a clinician can leave an application or file open on their desktop, leave the office, and resume working from their mobile device. With WorxDesktop, they can run an app that requires greater functionality (such as Flash capability) on their desktop but remotely control the app from their mobile device. This is a great example of Citrix and XenMobile offering unique ways to boost mobile user productivity while removing barriers that prevent anytime, anywhere, any device workspaces.

Complete enterprise mobility management: Creating a unified experience to harness the full potential of secure mobility in healthcare

For 25 years, many healthcare providers have relied on Citrix XenDesktop®, XenApp®, and NetScaler® to optimize and secure the delivery of applications like EMRs and imaging viewers and full desktops. Further, single sign-on capabilities are integrated into XenDesktop and XenApps so clinicians can access applications and other resources quickly from wherever

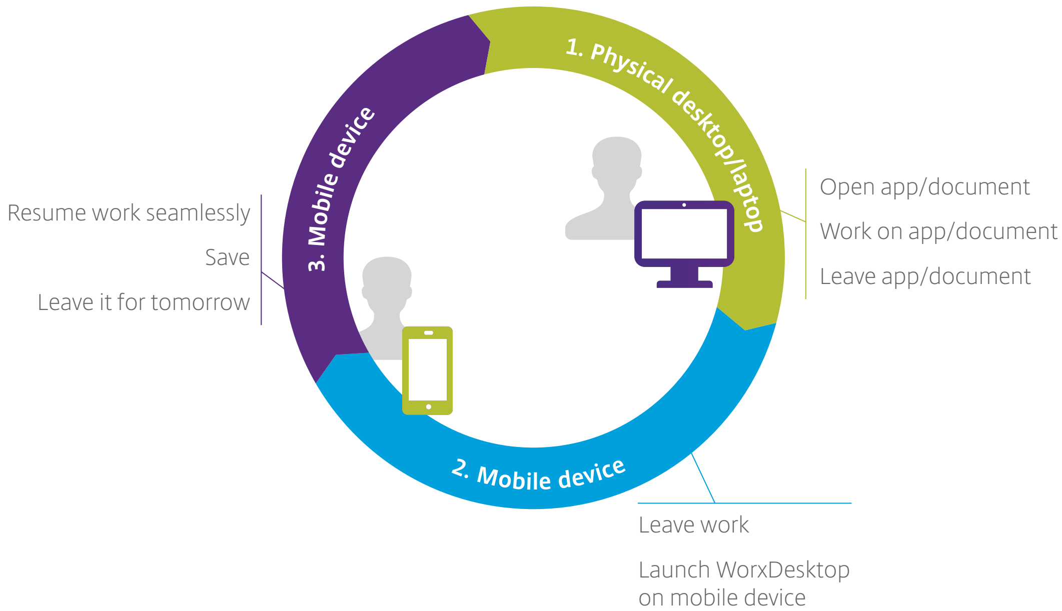

Figure 2. Sample workflow: "follow-me data and apps"

they're working. These products provide real-time access for mobile clinicians and staff and address remote access requirements because of the device-agnostic technology that allows Windows-based apps to be delivered to any device, anywhere, for all users.

XenMobile expands upon and integrates these proven healthcare IT products from Citrix with a complete EMM offering. By creating an integrated, unified corporate app store, clinicians get a single place to instantly access all of their clinical, business, and productivity apps – mobile, web, software-as-a-service (SaaS), and Windows – on any device. Users can easily choose the apps they need for their job and have them instantly available on their devices. As they move among their favorite devices, their chosen apps follow them to ensure optimal productivity in any scenario.

XenMobile also helps bridge the gap as IT moves legacy Windows-based apps onto mobile platforms. And the solutions we're pioneering, including the Worx App SDK and Worx App Gallery, are critical to developing future mHealth apps. The healthcare apps that you'll find in the Worx App Gallery, whether they are third-party developed apps or those created by Citrix, have all been Worx-enabled through the Worx App SDK. What this means is that developers have added a single line of code to their apps that acts like a conduit to app controls that have been enabled by the developer.

From an IT management perspective, scenario-based controls and identity-based provisioning help IT maintain security and control whenever, wherever, and on whatever device healthcare professionals use to access corporate apps and data –regardless of platform. Like Citrix XenApp and XenDesktop, XenMobile leverages existing corporate directory and authentication systems to provision, deliver, and control usage of mobile, intranet, web, and SaaS apps and data based on user identity and role as well as endpoint analysis. IT can instantly provision all of a user's applications and data as soon as the individual is added to Active Directory. Conversely, IT can immediately prevent access by specific users by disabling them or removing them from the directory system and closing their accounts.

Enterprise mobility management in the real world

Citrix healthcare customers already leverage XenMobile to solve mobile management challenges and empower people to use the full diversity of mobile devices, including personal devices and native mobile apps. By enabling healthcare executives, clinicians, and staff to be more productive on their mobile device of choice – anywhere, anytime – providers can transform business operations and care delivery.

Doctors can access patient records on a tablet while making rounds, use the tablet to show and discuss results of a CT scan at the patient's bedside, and consult face-to-face with hospitalized patients and their families from another facility. Nurses could view real-time monitoring data on a smartphone while moving from room-to-room or send a secure text message to better coordinate care during a hectic shift transition. On-the-go administrative staff could gather and process insurance and payment information from a tablet in real time, or collect critical quality metrics as they roam floor to floor. By ensuring that the appropriate level of access to apps and data is granted for each scenario, and that all clinical and patient data is secured and can be remotely locked or wiped, the solution supports HIPAA and PCI-DSS compliance requirements.

You don't have to lock down mobility to gain control

Given the paramount importance of security in IT's mission – as well as the heavy regulatory and ethical burdens of maintaining patient privacy – the natural instinct may be to try to lock down and limit people's choice of devices or otherwise constrain the endpoint environment, even if it means sacrificing the benefits of greater productivity and flexibility. But simply barring the door to consumer device usage and BYOD is neither realistic nor desirable.

It's inevitable that IT will face increasing pressure to provide access to any app, including innovative new mHealth apps, anywhere, on any type of device. Simply put, IT has no choice but to enable and support consumer mobile devices and BYOD; the only question is how.

The first response of many IT organizations to the influx of consumer-grade and employee-owned mobile devices has been to lock down and control every mobile device in the enterprise through MDM. But as mobile device types, operating systems, and apps proliferate, most IT organizations with MDM find that they're forced to impose limits on the mobile apps available on employee-owned devices to avoid increasing security risks and management complexity. Innovative mHealth apps, including Windows, web, and SaaS apps, remain unavailable, which severely limits opportunities for mobile productivity gains in healthcare. Citrix XenMobile provides a better way.

XenMobile enables a better, more productive experience

This is the most complete EMM solution available to healthcare providers, clinicians, and patients: providing mobile device, application and data management, as well as enterprise-grade productivity apps in one comprehensive solution. And it enhances the user experience on BYO or hospital devices without compromising security.

XenMobile helps fulfill IT's new mission to usher in the most advanced mHealth applications that can cost-effectively provide better outcomes for patients. And it meets the expectations of younger clinicians for a mobility-enhanced work environment.

The EMM solution, working with powerful, built-in mobile apps, provides immediate value and encourages buy-in from powerful mobile users like healthcare executives and clinicians. Citrix XenMobile unites these mobile device and app capabilities with all of the other tools people use daily, such as Windows desktops and apps and files, to enable the highest level of adoption and long-term productivity for a healthcare provider's mobile clinicians, staff, and executives.

Additional resources

For more information, please look at these additional resources.

Website: www.citrix.com/xenmobile and www.citrix.com/healthcare

White paper: The 10 "must haves" for secure enterprise mobility

Customer Story: Franciscan Missionaries of Our Lady Health System

HOWARD™ med
TECHNOLOGY SOLUTIONS

General Information: 1 (888) 912-3151
Web: www.howard-medical.com

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.