THE BLACKBERRY GUIDE TO MOBILE HEALTHCARE

Strategies, Tactics, and Case Studies for CIOs and other Leaders

BlackBerry®

THE BLACKBERRY GUIDE TO MOBILE HEALTHCARE

Strategies, Tactics, and Case Studies for CIOs and other Leaders

The BlackBerry Guide to Mobile Healthcare: Strategies, Tactics and Case Studies for CIOs and other Leaders.

Published by BlackBerry Ltd. 2200 University Ave. E Waterloo, ON, Canada N2K 0A7

To download PDF or e-book copies of The BlackBerry Guide to Mobile Healthcare,
visit http://web.blackberry.com/enterprise/industries/healthcare.html
Copyright © 2015 BlackBerry Ltd. All rights reserved.

BlackBerry and the BlackBerry logo are trademarks of BlackBerry, Ltd. or its subsidiaries.
® indicates registration in the United States. All other trademarks are the property of their respective owners.

U.S. Library of Congress Cataloging-in-Publication Data

BlackBerry Ltd. The BlackBerry Guide to Mobile Healthcare.

Edited by Sarah Burt, Sara Jost, and Eric Lai.
p.cm.
ISBN 978-1-943842-37-7
1. Healthcare IT. 2. Enterprise Mobility. 3. Information Technology. 4. Mobile Healthcare.

U.S. Library of Congress Class and Year: TK5103.2 .H84 2015
Library of Congress Control Number: 2014946844

Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Thanks to:
Project manager: Jill Thater
Copy editors: Carla Thornton, Giovanna Heffernan, Karen Grierson
Designers & Printers: The PD Group – thepdgroup.com
Executive Sponsors: Marty Beard, Mark Wilson, and Jennifer Doidge
Read Bizblog.BlackBerry.com, and follow us at Twitter (@BlackBerry4Biz),
LinkedIn.com/Company/BlackBerry and SlideShare.net/BlackBerry

BlackBerry

Table of Contents

Foreword

Chapter 3

Developing Your Mobile Strategy

Chapter 4

Cross Platform EMM

Chapter 5

Clinical Collaboration

Chapter 6

Staff Coordination

Chapter 7

Home Care

Chapter 8

mHealth

Chapter 9

Connecting and Securing the Healthcare Internet of Things (IoT)

Mobility Offers Huge Potential Benefits for Healthcare. Let's Take Advantage of Them.

By John S. Chen
Executive Chairman and Chief Executive Officer,
BlackBerry Ltd.

Healthcare, as in many fields, has adopted mobile technology in vastly uneven ways. On the one hand, hospitals and clinics have been among the biggest champions of Bring-Your-Own-Device for its workers. One survey in 2014 found that 70 percent of nurses and a whopping 96 percent of doctors use personal smartphones while providing patient care.

That's great, until you start to consider the many data security regulations that healthcare organizations operate under – and how unmanaged or weakly-managed BYOD puts data at increased risk. 52 percent of healthcare IT leaders reported an increase in mobile breaches in the prior 12 months, according to a global governance, risk and compliance survey conducted last year by BlackBerry. 63 percent of healthcare IT respondents told us that mobility was their business's Achilles Heel. And only 28 percent were very confident that their data assets are protected against unauthorized mobile access.

As a result, 65 percent of healthcare IT leaders were very concerned about reputational damage, while 52 percent pointed to lawsuits and litigation as worries. Financial penalties (47 percent) and lost revenue (37 percent) also scared healthcare leaders as well.

Besides underinvesting in security, many healthcare organizations haven't embraced the mobile advances that would maximize their efficiencies and productivity. They might not have put their patient medical records into electronic form accessible via mobile devices. They may not have deployed an enterprise mobility management (EMM) platform that can serve as the nerve center for overseeing all of their mobile devices. They may not be deploying the right mobile health apps, or not have gotten buy-in from staffers or trained them properly on new technology.

There is plenty that most healthcare organizations can still do. What's your game plan? To help you create one, I would suggest starting by reading this guide book, The BlackBerry Guide to Mobility in Healthcare: Strategies, Tactics and Case Studies for CIOs and other Decision Makers.

This guide offers strategies and advice by BlackBerry security and healthcare experts, experts at partners such as Cisco Systems, SAP, Lexmark, and others, analysts at Machina Research, as well as actual CIOs and other experts at healthcare organizations similar to yours. There are also a dozen case studies detailing the ROI that hospitals and clinics are gaining from going mobile.

After reading this guide, I invite you to download our other e-books. *The Definitive Guide to Enterprise Mobile Security* ➋ is a primer for business and IT decision makers on all of the mobile threats – and solutions – that they need to know about. *BlackBerry Customer Success Stories* ➋ is a 240-page guide featuring 50+ case studies of successful mobile enterprises, including many healthcare organizations.

I also invite you to visit *BlackBerry.com/healthcare* ➋ to download other informative resources, follow BlackBerry via blog and social media to learn more tips on enterprise mobile security, and continue the conversation with one of the healthcare and mobile experts here at BlackBerry.

BlackBerry®

Chapter 1

The Changing Face of Healthcare

Mobile Medicine: How Mobility is Changing Healthcare

By Marty Beard, Chief Operating Officer, BlackBerry

Mobility is changing the way healthcare is delivered. Today healthcare professionals use smartphones and tablets to do everything from remotely updating patient records to diagnosing conditions and monitoring sensor-equipped equipment in the patient's hospital room. Connected medical personnel use a wireless network of mobile devices to communicate and collaborate with their colleagues down the hall and around the world. Home healthcare workers are using mobile devices to access and update patient care plans in real time as they complete their visits. Patients are being monitored remotely using diagnostic devices connected to smartphones. These are exciting times.

And the benefits of mobilizing healthcare are plentiful. Real-time remote monitoring, the tools to collaborate instantly with colleagues, and the ability for clinicians to spend more time at a patient's bedside instead of chasing down information all improve the quality of patient care and ultimately lead to better patient outcomes. It also results in increased satisfaction for both patients and healthcare providers alike.

In this book, we will look at the current technological state of mobile healthcare, how we got here, and where we're going. We'll help you create a mobility strategy and explain how you can manage mobile devices using the right software, how to streamline your workflows and processes, and improve your relationship with patients. We'll examine the advantages and disadvantages of BYOD and other mobile deployment strategies, how to approach risks and liabilities, and how to learn from other organizations that have already successfully implemented various mobile technologies. And we'll also give you a primer on the next wave of healthcare innovation – the healthcare Internet of Things (IoT) – and how some cutting-edge organizations are already taking advantage.

> "Healthcare professionals use smartphones and tablets to do everything from remotely updating patient records to diagnosing conditions and monitoring sensor-equipped equipment in the patient's hospital room."

ONLY 1 IN 4 HEALTHCARE ORGANIZATIONS ARE VERY CONFIDENT

that their data assets are protected from unauthorised access via mobile devices

Source: BlackBerry Mobility Risk Tolerance Survey, Sept. 2014

FACT BOX

Data Breaches, Hack Attacks and Damages on the Rise

Criminal attacks in healthcare are up 125% vs. 5 years ago

Medical identity theft has doubled in last 5 years, to 2.3 million adult victims in 2014

Average cost of data breach per organization is $2.1 million

Data breaches cost healthcare industry $6 billion per year

Criminals cause 45% of healthcare data breaches and are the leading cause of breaches

65% of healthcare organizations had electronic information-based security incidents in last 2 years

Yet, more than 50% of healthcare organizations say their incident response process is weak, while 33% lack a process altogether

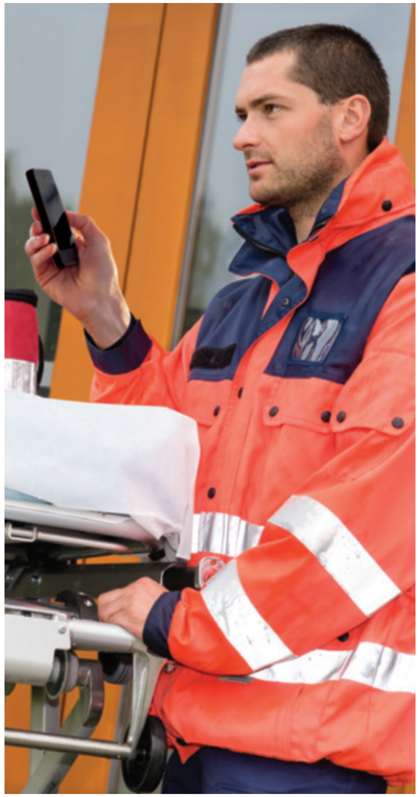
Source: Ponemon Institute, May 2015

From Faxes to EHRs

Remember the first mobile phones? Just 20 years ago they were bricks compared to today's handhelds, and users could only make voice calls. Faxes were the fastest way to transmit a file from one medical center to another. Videoconferencing in the operating room was almost unheard of, short of mounting a TV camera above the operating table.

Until recently, hospitals and clinics stored all medical records on paper, X-ray film, and other physical media. Old files often were archived off-site and took 24 hours or longer to retrieve. Worse, if patients arrived at a hospital that didn't have their medical records, they had to wait for the attending physician to contact their regular doctor to fax or overnight the needed files.

Now, electronic medical record software systems allow clinicians to instantly access computerized patient charts along with lab test results, CT scans, and MRIs from their mobile devices, whether the patient is local or being treated on the other side of the world. Specialists in remote locations can easily consult on a patient case if necessary, and nobody has to sit at a desk to do it – mobile devices let medical personnel work whenever and almost anywhere they need to.



One medical community that has embraced smartphones are first responders. The high-definition cameras built into today's consumer-grade smartphones take incredibly sharp images of accident victims and other patients that can be immediately sent to emergency room doctors. No longer are physicians limited by the first responder's verbal description of a problem or the vitals scan written down on paper and then transmitted wirelessly back to the hospital.

In its *Connecting Health and Care for the Nation: Nationwide Interoperability Roadmap* report issued in 2014, the US government's Office of the National Coordinator (ONC) for Health Information Technology made a bold prediction: "With the emergence of Internet-accessible medical devices, monitors, and the yet-to-be-developed Internet of Things, it is not too far-fetched to imagine a time in the near future in which a mobile device may be used to identity proof and authenticate a patient and their associated devices at the point of care."

> "First responders are using smartphones to take and transmit incredibly-sharp images of accident victims and other patients to ER doctors to give them better information prior to their arrival."

63%

of surveyed healthcare organizations believe mobile devices are the

WEAKEST LINK IN THEIR ENTERPRISE SECURITY FRAMEWORK

Source: BlackBerry Mobility Risk Tolerance Survey, Sept. 2014

Besides authenticating patients for the hospital of the future, the ONC sees mobile devices as doing more. Healthcare organizations must “become more agile and leverage the experience” of mobile apps “such as those created by Facebook, Amazon and Apple,” in order to enable patients to “integrate data from their health records into mobile apps and tools that enable them to better set and meet their own health goals.”

Bypassing Roadblocks

Of course, not every medical center can have all the latest mobile technology at its disposal. Many facilities simply can’t afford every new technological advancement, while others don’t have the staff or IT expertise to implement it. Almost all organizations face some internal resistance: clinicians, administrators, or corporate management who aren’t sure of change. Management might be unfamiliar with the advantages of a new technology or fear that a cutting-edge system will be too disruptive or somehow put them at risk of violating a patient’s privacy or data security.

Let’s look at some of these lingering concerns and how healthcare organizations are overcoming potential objections.

Will My Patients Approve?

Few changes in technology have inspired more anxiety in the medical community than patient electronic health records (EHRs). One legitimate fear was how patients might react to having their personal medical information stored and shared on computer networks instead of paper. If patients did overly fear EHRs in the beginning, a recent ONC report, *Individuals’ Perceptions of the Privacy and Security of Medical Records,* suggests that the initial concerns have subsided. In both 2012 and 2013, fewer than one in 10 patients withheld information from doctors due to security concerns, and three out of four patients wanted their doctors to use EHRs and share their medical information with other doctors over health information exchange (HIE) networks.

Patients’ growing acceptance of EHRs and HIEs suggests that they feel similarly about doctors doing business over smartphones, a technology that patients themselves already feel comfortable with.

Will My Workflow Suffer?

A concern that healthcare providers have about implementing new technology is how it will affect their own work. There are plenty of moving parts that require the attention of the IT, security, and operations departments, not to mention staff in general. This concern about how the new technology will affect their work makes the adoption of new technology a challenge for everyone. Any medical practice that has switched to EHR software can attest to the time it takes to work out the bugs.

Having a roadmap is essential. Long before you change or add any network infrastructure in anticipation of upgrading your mobile capabilities, your IT team should evaluate its healthcare reference architecture to ensure all the basics are in place. Your reference architecture is a template of how you will build out your mobile technology. It's the blueprint from which you will select best-of-breed products and services and create the policies and procedures to ensure that everything works together. Here are a few of the basics your reference architecture should have:

- An Enterprise Mobility Management (EMM) application in place that can manage a variety of mobile platforms. Products such as BES®12, BlackBerry's cross-platform EMM solution, serve as the nerve center of your mobile management strategy by tying together diverse operating systems, applications, and data management functions.
- A mature network and data security strategy in place that addresses identity, credentials, and access management, patch management, antivirus and anti-malware capabilities, and encryption. The network and data security strategy should cover both wired and mobile users.
- Written information security policies and procedures that users can access any time.
- Buy-in from the hospital's clinical, executive, technical, operations, and nonmedical staff. Sometimes installing new technology is the only way to see a dramatic increase in productivity in the long run. "This is the way we've always done it" can't be allowed as a response to solving problems.

Finally, your reference architecture should ensure that you opt for mobile devices and software whenever they improve workflow and patient care. Fixed, permanent, and dedicated equipment is certainly part of the equation. Wherever possible, though, consider mobile devices. Mobile and embedded devices can ensure that patients get the care they need wherever they – or their healthcare providers – happen to be.

> Hospitals will soon use data generated from monitoring the patient's room, from the height of the bed rails to the air temperature to the status of all medical devices, to issue alerts to doctors and nurses and otherwise improve care.

Standards and Compliance

Before implementing new mobile technology, medical organizations should ensure regulatory compliance. While most healthcare data breaches involve a relatively small percentage of employees or patients, the resulting monetary penalties and bad PR can hurt your entire organization. Major breaches such as the cybertheft of up to 80 million patient records that the insurer Anthem suffered in January 2015 can leave a long-lasting negative association in the public mind.

Depending on your jurisdiction, double-check your organization's compliance with regulatory standards such as the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 2009 Health Information Technology for Economic and Clinical Health (HiTECH) Act and the 2004 Personal Health Information Protection Act (PHIPA), which include a number of requirements for patient information security. While these rules could require some investment in new technology, you might have already made the switch to EHRs, computerized physician order entry for medication, and other required electronic advances. That means much of the basic infrastructure might already be in place for you to take the next step: a secure, fully connected hospital. This is the future enabled by the Healthcare Internet of Things.

Connected Healthcare in Hospitals

Already, hospitals are testing how they will connect virtually all aspects of their hospital operations in order to provide safer, faster care while protecting patient privacy. Embedded systems will monitor heating, ventilation and air conditioning systems, and tie them to the hospital's electrical grid. Data generated from monitoring the patient's room, from the height of the bed rails to the air temperature to the status of all these IoT-enabled medical devices, will stream into a software program that aggregates information and issues wireless alerts to the appropriate doctors and nurses.

Eventually hospitals will use identity and access management software that identifies both the user and the device. Multifactor authentication is a different approach that authenticates the user using a combination of password, hardware or software token (for example, on a mobile device app), or biometrics such as fingerprints. The mobile device itself also can have multiple layers of authentication that software such as BES12 manages, ensuring that the credentials of the user and the device match the required security level to access private data.

In the meantime, mobile devices can help you improve care now. A huge part of hospital operations is reducing treatment risks – risk of complications that patients might experience while their physician is analyzing their symptoms, risks of adverse drug reactions, and much more. Mobile technology can play a major role in reducing risk. For instance, having mobile access to a patient's entire chart, complete with a photograph of the patient's face and a list of all of her allergies, ensures that doctors have the right chart for the right patient, even if the patient's physical chart is stored at a different medical facility.

Total Cost of Ownership

The total cost of ownership (TCO) of technology ties together not only the cost of the physical infrastructure but also the expenses associated with implementing, supporting, and maintaining the technology. The TCO of a highly-mobile work force, which requires less physical infrastructure and gives people greater work flexibility, looks great on the bottom line, but there is more to it than just operational savings.

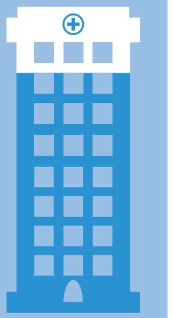
As you increase technological efficiencies, you also increase the value each member of the staff delivers directly to patients and operations. For instance, a system that alerts nurses if an IV needs to be changed or the bed rail is down for a patient at risk for falls, means that the patient gets better care and nurses are more productive. Mobile technology is more than just another way of delivering a service to a patient. Mobile technology changes the playing field so that each person in the continuum of care, from the first responder on the scene of an accident to the clinician who walks from room to room carrying each patient's full chart on a tablet, can deliver the best care possible because they have all the data that they need at their fingertips.

As a result, the costs associated with buying new hardware and software can be spread much further throughout the organization, while reducing both the medical risk to the patient and the technological risk to the network. The IT costs related to system configuration, maintenance, and support will decrease as your IT team will be able to do much more work remotely. No longer is it necessary to touch every system in order to do software upgrades or security maintenance; much of this work can now be done remotely as well, saving you the cost of dispatching an IT technician to physically visit every system.

Go Ahead, Bring Your Own Device

Bring Your Own Device (BYOD), the device deployment model where workers use their own smartphones on the job, has been both a benefit and a dilemma for most healthcare organizations. Surveys by *Spyglass Consulting Group* show that 96 percent of doctors and 70 percent of nurses have used their own personal devices at work. Although BYOD might seem like a great way to reduce capital expenses, the security trade-off occurs when employees mix personal information with HIPAA-protected hospital and patient data on devices that your IT organization doesn't control.

FOUR-FIFTHS (81%) OF EXECUTIVES AT HEALTHCARE PROVIDERS AND PAYERS SAY THEIR INFORMATION TECHNOLOGY HAS BEEN COMPROMISED BY CYBER-ATTACKS IN THE PAST TWO YEARS.



Source: KPMG Healthcare Cybersecurity Survey, 2015

Corporate Owned, Personally Enabled (COPE) and Corporate Owned, Business Only (COBO) mobile device programs are becoming popular alternatives to BYOD because they better protect company data and can be easier to manage. Whether you allow BYOD or want to implement COPE or COBO – or a mix of all three – BES12 can manage BlackBerry, iOS, Android, and Windows Phone smartphones and tablets.

Mastering Mobile Communications

Many hospitals today augment some traditional, permanent computer systems with a wireless mix of mobile devices and embedded systems. Medical personnel can provide care directly to the patients and monitor both the environmental and physical aspects of hospital rooms in real-time.

The next steps your institution takes require vision, creativity, and trust that the technology you use is advanced enough to successfully implement your mobile device strategy. BlackBerry and its technology partners are implementing those advanced technologies today. With BES12, BlackBerry offers a reliable foundation upon which healthcare facilities can build the innovative medical centers of tomorrow.

When you have mastered your organization's communications infrastructure – when voice, data, and images can be securely transmitted among first responders, hospital staff, and home healthcare providers, and every participant in the healthcare continuum is connected with colleagues and to medical equipment – the only limits to how you provide healthcare is your creativity.

Read on for more information about how BlackBerry can help you achieve your healthcare mobility goals.

Marty Beard is Chief Operating Officer at BlackBerry and is responsible for leading cross-functional operations, including Marketing, Pricing, Application Partnering, Manufacturing & Supply, Customer Care and Quality. He is also responsible for instituting best practices and processes across the organization to ensure operational excellence.

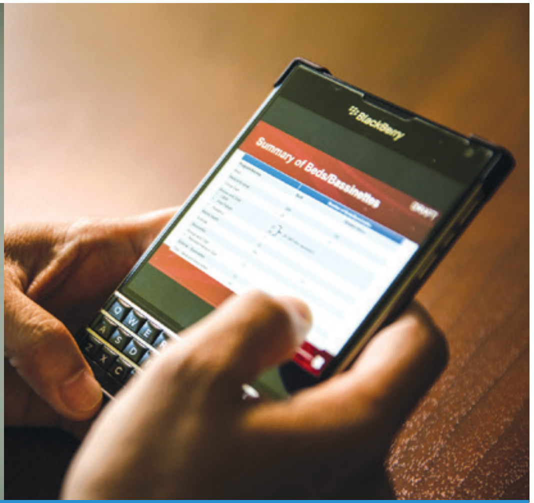
Healthcare of the Future: The Mackenzie Health Innovation Unit

By Tiziana Rivera, Chief Nursing Executive and Chief Practice Officer, Mackenzie Health

At Mackenzie Health, patients are at the center of everything we do. To provide the best patient-centered care, the organization has embarked on an Innovation Journey where collaboration, partnerships, and evidence-based practice set the stage to provide an excellent care experience. Mackenzie Health views innovation as a key factor for our organization going forward. We strongly believe that leveraging healthcare technology and partnerships with industry leaders will help us achieve our vision to create a world-class health experience for our community.

Mackenzie Health brings together advancements in mobile communications with innovations in medical diagnostic and monitoring technologies, as well as the recognition that medical professionals are at their best when delivering high-quality care at the patient's bedside. The result is our Innovation Unit, a first-in-Canada project that features a unique integration of advanced technology to transform the delivery of care.

The Innovation Unit is an acute care medical unit that has been transformed into a living and breathing laboratory to develop, evaluate, and introduce innovations into other patient care units. In the first phase of the Mackenzie Innovation Institute (Mi2) project, we implemented technologies such as "smart" beds that use wireless sensors to track patient presence, weight, position of side rails, brakes, and height of beds to alert caregivers when patients are at risk of unsafely exiting the bed. We also introduced technology that monitors hand hygiene that tracks how often doctors and nurses wash their hands and alerts them if they forget to do so. "Smart" badges quickly locate staff using sensors that track their real-time location on the patient unit. These innovations all support and create safer and more effective patient care.



> Mackenzie Health brings together advancements in mobile communications with innovations in medical diagnostic and monitoring technologies, as well as the recognition that medical professionals are at their best when delivering high-quality care at the patient's bedside.

As we enter Phase Two of the Innovation Unit, we will implement a smart mobile clinical messaging and alerting system, using intelligent automation rules between information systems and devices to improve processes at the point of care. Our business partners for this phase of the program – BlackBerry, Cisco Systems and ThoughtWire, along with funding from the Ontario Centers of Excellence and the Ministry of Government and Consumer Services – are joining forces to create the next generation of quality care using the most advanced mobile communications, networking, and medical device management software available.

Cisco is the gold standard in networking technology. BlackBerry is a world leader in secure and private mobile communications. And ThoughtWire's Ambiant™ platform and experience in device integration and machine intelligence enables the clinical process improvements.

Phase Two leverages innovations in pervasive computing – computers embedded in everyday objects to communicate information directly to key medical personnel. The solution uses ambient intelligence, such as electronic environments that are sensitive and responsive to the presence of people, to create a contextually aware and personalized experience that anticipates staff and patient needs.

Most errors in healthcare occur because critical data that already exists in hospital information systems was unavailable to medical professionals at a critical point in time.

> Most errors in healthcare occur because critical data that already exists in hospital information systems was unavailable to medical professionals at a critical point in time.

> The "smart" environment in the Innovation Unit will be able to anticipate the needs of the medical professionals and the patients, and deliver information to healthcare providers quickly, efficiently, and safely.

Our goal is to deploy these advanced mobile technologies to provide critical patient data to the doctors and nurses at exactly the moment they need it. The "smart" environment in the Innovation Unit will be able to anticipate the needs of the medical professionals and the patients, and deliver information to healthcare providers quickly, efficiently, and safely.

There are three main goals in this second phase. The first is to provide faster, more accurate, and secure communications between patients and their healthcare providers. The second is to enable more informed decisions by healthcare professionals at the patients' bedside. The third is to ensure safer and more efficient patient care. All three goals are achievable and reasonable given the advanced technology we have in place and what we plan to deploy.

Mackenzie Health will analyze the information collected through this process of progressive implementation and evaluation in the real-world hospital environment. The data will inform planning decisions for the construction of the Mackenzie Vaughan Hospital, as well as at the provincial healthcare system level and beyond.

That said, this is not just a demonstration project. We are serving real patients right now in the Innovation Unit. Mobile communication makes these transformative advancements possible. Giving healthcare professionals the very latest data in real time reduces potential introductions of erroneous or unnecessary data.

We look forward to completing this phase of the Innovation Unit and demonstrating how high-quality healthcare can and will be delivered in the very near future.

As Chief Nursing Executive & Chief Practice Officer and a member of the Senior Leadership Team at Mackenzie Health, Tiziana Rivera provides strategic leadership for the development and implementation of a shared vision for interprofessional practice, quality, safety and patient-centered care.

Chapter 2

Mobility Risks in Healthcare

Why Mobile Security Could Be Your Organization’s Weakest Link

By Suzanne Riddell, Director, Advanced Security Solutions, BlackBerry

Your organizational security is only as strong as its weakest link – and in healthcare, evidence suggests that the weakest link is mobile security. The *Mobility Risk Tolerance: Closing the Gap in a Mobile First World survey* carried out last year by BlackBerry saw 63 percent of respondents in healthcare pointing at mobile security as their business’s Achilles Heel. The question is, why?

What is it about mobile technology that makes it so difficult for healthcare IT to manage – and how can decision makers address this?

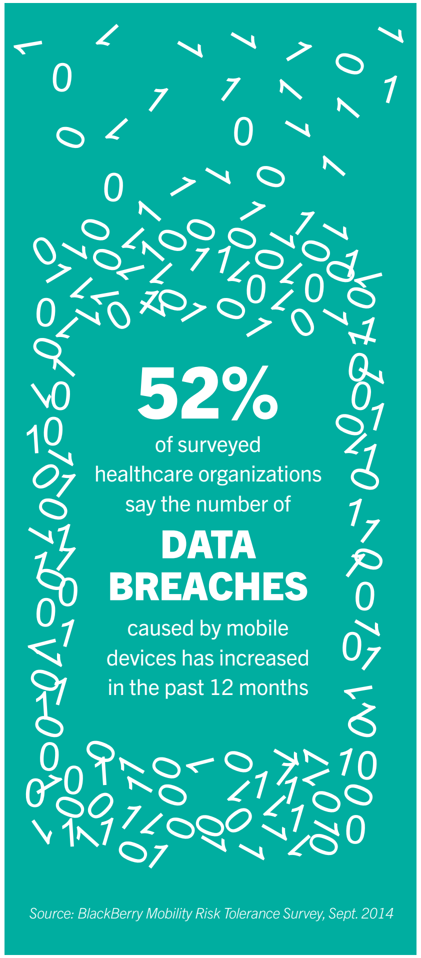
Mobile devices have become ubiquitous in hospitals and healthcare organizations, but many organizations have failed to adequately support them. Frustrated by a lack of IT support, an increasing number of healthcare professionals have turned to personal mobile devices for clinical communication. Although the use of personal devices exposes their organizations to a whole gamut of risks, the potential productivity gains simply represent too great a payoff to ignore.

A 2014 research report by Spyglass Consulting Group found that nurses at 70 percent of hospitals use personal smartphones for point-of-care collaboration. *Another report released by Spyglass Consulting Group* later that year found the number to be even higher among physicians, at 96 percent, while 70 percent of respondents indicated that they believe that their in-house IT support isn’t doing enough to address increasing mobile usage.

IT is aware of the risks and challenges of mobile compliance. Referring back to the compliance survey, 73 percent of healthcare respondents felt that their business is more risk-tolerant than is acceptable, while 52 percent reported seeing an increase in data breaches over the prior 12 months. It’s unsurprising that only 28 percent are very confident that their data assets are protected against unauthorized mobile access, while only one in four are happy with their current mobility risk management solutions.

The key issue here is that smartphones and tablets have brought about sweeping changes in an industry whose communication technology has changed relatively little over the past several decades. CIOs and their colleagues are expected to strike a delicate balance between regulatory compliance and the needs of their end-users for mobility, and 8 of 10 respondents feel that this is an increasingly difficult task with little guidance to help them along.

But it’s also a balance that healthcare leaders need to achieve. Otherwise, they leave their organizations wide open to a data breach, which could have disastrous results. 65 percent of survey respondents said they were very concerned about reputational damage, while 52 percent pointed to lawsuits and litigation as serious threats. Financial penalties (47 percent) and lost revenue (37 percent) also worry healthcare technology leaders.



52% of surveyed healthcare organizations say the number of **DATA BREACHES** caused by mobile devices has increased in the past 12 months

Source: BlackBerry Mobility Risk Tolerance Survey, Sept. 2014

> 70% of nurses and 96% of doctors use their personal smartphones to help them provide better care.
>
> *Source: Spyglass Consulting*

Where can IT start in preventing this? By carrying out a risk assessment and identifying all mobile-based threats to the security of protected health information, healthcare organizations can begin formulating a compliance program that addresses potential threats and concerns. These risks may include:

- **Device theft/misplacement:** A lost or stolen device can provide access to Personal Health Information (PHI) and medical applications; much of the data recovered in this way may end up sold on the black market.
- **Lack of encryption:** Without proper protection, mobile communications are subject to eavesdropping and can leak confidential information to an unscrupulous third party. Unencrypted emails, unprotected data traffic, unencrypted chat messages, or connections through unsecured networks are all subject to eavesdropping and data leakage.
- **Unauthorized applications:** *eWeek reported in 2013* about a survey that found that more than eighty percent of the top Android and iOS apps leak information in some way, shape or form, and mobile malware was on the rise. Therefore, untrusted applications represent a serious threat because they can offload sensitive data, either inadvertently or by design.
- **Employee disclosure:** Employees may disclose sensitive data, either through ignorance or malice – for example, sending private patient data through a P2P messaging app or emailing health records to an outside party.

After a risk assessment has been carried out, mitigation comes next. In order to take care of both compliance requirements and the end user, healthcare providers require an Enterprise Mobility Managemet (EMM) suite that secures every part of their mobile infrastructure, including physical devices, applications, and both data in transit and data at rest.

An effective EMM solution must also have a number of high-assurance techniques in place to help manage risk, such as automated testing, failure and vulnerability analysis, and formal safety and security enforcement methods. Containerization is a requirement, as well. By separating work applications and data from an employee's personal use of their phone, IT departments eliminate the need for staff to carry two devices. Thus, containerization allows a business to support a BYOD model without compromising either compliance or patient privacy.

Risk assessment and EMM aside, the respondents to the BlackBerry survey feel that their organizations should take the following steps when developing their risk-management strategy:

- Involve governance, risk, and compliance (GRC) teams in the decision-making process (63 percent)
- Update vendor selection methods based on the current risk/mobility landscape (68 percent)
- Consider adopting a COPE (corporate owned, personally enabled) deployment model either now (57 percent) or in the next two years (50 percent)

The healthcare communications landscape has changed, and it's time for healthcare providers to change with it. Neither security nor convenience can be an afterthought any longer – decision-makers must consider both up front when mapping out mobile infrastructure and workflow. Security without convenience will impede users, and they're likely to find workarounds that potentially conflict with compliance. Convenience without security exposes an organization to possible data breaches that might be grounds for litigation and regulatory action.

There needs to be a balance; otherwise, healthcare organizations will never be capable of strengthening their weakest link.

Suzanne Riddell is Director of Advanced Security Solutions and is responsible for the Security Program Management Office and Security Certifications programs at BlackBerry.

How to Identify Mobile Risks and Understand the Key Threats

By Alex Manea, Director, BlackBerry Security, BlackBerry

Any strategy to mitigate mobile security risks has to start with a thorough evaluation and understanding of your organization's threat profile. Healthcare organizations are required by regulations like HIPAA and the HITECH Act to ensure that adequate controls are in place to protect the privacy and security of sensitive Protected Health Information (PHI) of their patients. The requirements extend to mobile computing just as they do to any environment that is used to store, share or access PHI. In order to mitigate mobile risks, organizations need to look beyond device-level protection and focus on the entire enterprise mobility landscape.

In order to create an effective strategy to mitigate mobile security risks for your organization, you need to:

- Know how much of your sensitive data is accessible from personally owned smartphones, tablets and other mobile computing devices
- Determine if you can adequately defend yourself against cyber-attacks and limit the impact of data loss incidents caused by a malicious acts or by lost or stolen devices
- Implement the appropriate security controls to mitigate risks while still enabling the key productivity and efficiency benefits of enterprise mobility

Let's examine each one of these factors more closely.

> In order to mitigate mobile risks, organizations need to look beyond device-level protection and focus on the entire enterprise mobility landscape.

Know What To Defend

A fundamental concept in security is that you can't defend what you don't know about. To implement the right controls, you need to determine the extent of your vulnerability exposures and quantify the potential impact of a data compromise.

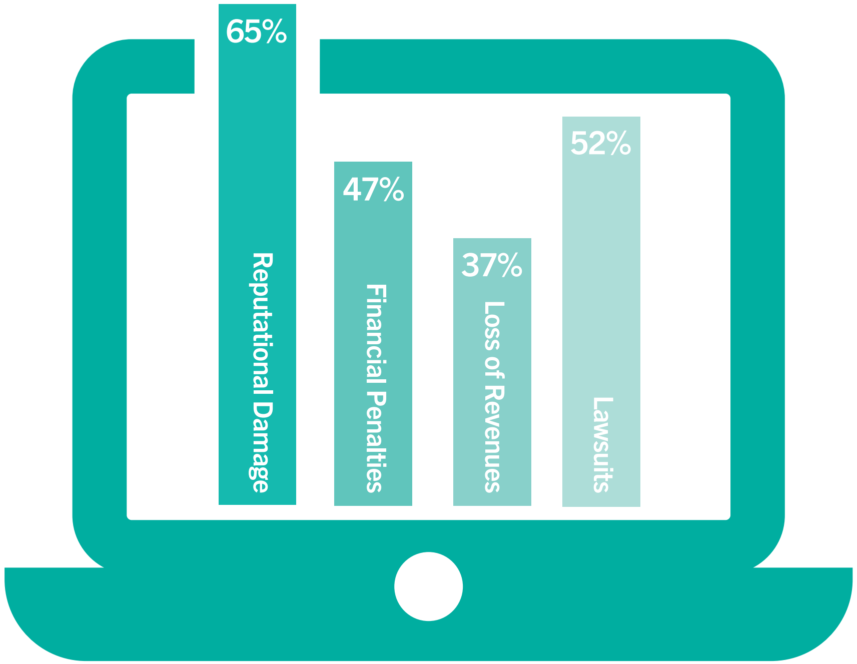
In a recent BlackBerry global survey of 800 business leaders on the risks and opportunities presented by mobility, 61 percent of the respondents said their organizations underestimate or miscalculate mobile risk by focusing purely on device security. Nearly three-quarters said their biggest concern with enterprise mobility is data loss from lost or stolen devices.

The reality is that mobile security risk extends well beyond the device itself. Unapproved or misconfigured applications and cloud services running on a personally owned device can pose serious security threats to PHI stored on the same device or to any business data that is accessed from the device. Analyst firm *Gartner* believes that by 2017, nearly 75 percent of mobile security breaches will result from mobile application misconfiguration.

Mobile malware is also rapidly evolving. There is every indication that cybercriminals will attack mobile platforms with the same ferocity with which they have attacked desktop and server environments for decades. This is especially concerning given that mobile operating systems are typically not updated as frequently as fixed IT systems and laptops. Mobile devices are, in many ways, more vulnerable than their fixed counterparts to threats like unauthorized monitoring and surveillance, data theft and misuse. The tendency by mobile device owners to jailbreak or root their devices in order to run unauthorized applications on them only exacerbates the situation. As Gartner notes, rooting or jailbreaking a device can make it vulnerable to malware downloads and heightens the risk of data extraction and loss.

Effective security requires you to consider all of these factors when determining your risk exposure. Before you can begin implementing controls, you need to know what, how, where and when your sensitive data is at risk. Who and how many people have access to PHI from their mobile devices? How much access do they have? What are they able to do with the access? Do they use personal devices to store and share protected health data?

Key Concerns of Healthcare Organizations in Event of a Mobile Breach



Source: BlackBerry Mobility Risk Tolerance Survey, Sept. 2014

MOBILE BEHIND HEALTHCARE'S INCREASING DATA BREACH ILLS

44% Healthcare accounted for 44% of all data breaches in 2014

68% 68% of healthcare data breaches since 2010 are attributed to lost devices or files

Source: Health and Human Services records. Ponemon Institute (2014)

Identify The Gaps

After you have a handle on your mobility risk exposure, you need to identify the gaps that exist in your security. What kind of device deployment environment do you have? Is it Bring Your Own Device (BYOD), Choose Your Own Device (CYOD), Corporate Owned Business Only (COBO), Corporate Owned Personally Enabled (COPE) or a mix of everything?

Over the years, enterprises have adopted a variety of mobility deployment options to address issues such as user choice, regulatory compliance, centralized control and productivity benefits. Whatever mobility deployment model you choose, you should evaluate the extent of your control over the mobile environment. Unless all of the mobile devices in your workplace are completely corporate owned and meant purely for business use, chances are high that they are being used for personal purposes as well.

Here are some other things to consider:

- Do you have the ability to properly segregate work and personal data?
- Do you have formal processes for registering, provisioning and de-provisioning mobile users from your network?
- Can you monitor and audit access to PHI from smartphones and tablets?
- Can you patch security vulnerabilities and issue updates over the air?
- Can you accommodate changes in workflow as more applications become mobile?
- What happens to mobile data when an employee leaves the company?

Choosing The Right EMM Platform

A plethora of Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) technologies are available that try to help enterprises address such questions and to exercise centralized control over the mobile landscape. But not all of them are created equal.

When evaluating MDM and EMM technologies, you should consider not only the available security features but also other factors like cross-platform management, cost, productivity enablement, compliance, analytics and, of course, support for your specific deployment needs.

Many organizations are forced to deal with highly heterogeneous mobile environments, often because they evolved that way organically. Any EMM solution that you choose needs to be able to support multiple platforms, device types and operating systems. It should enable centralized management of tasks like user account provisioning, policy management, email profiles, remote setup and software configuration, wireless software updates and remote wipe.

A robust EMM platform needs to be able to handle mobile application management tasks including secure application deployment, and to ensure that only approved applications are available for download on a corporate device. The solution should securely segregate approved business applications from any personal applications and data that might coexist. If your organization has compliance or other reporting obligations, it's vital to have an EMM platform that can report, monitor and audit all access to protected and sensitive health data.

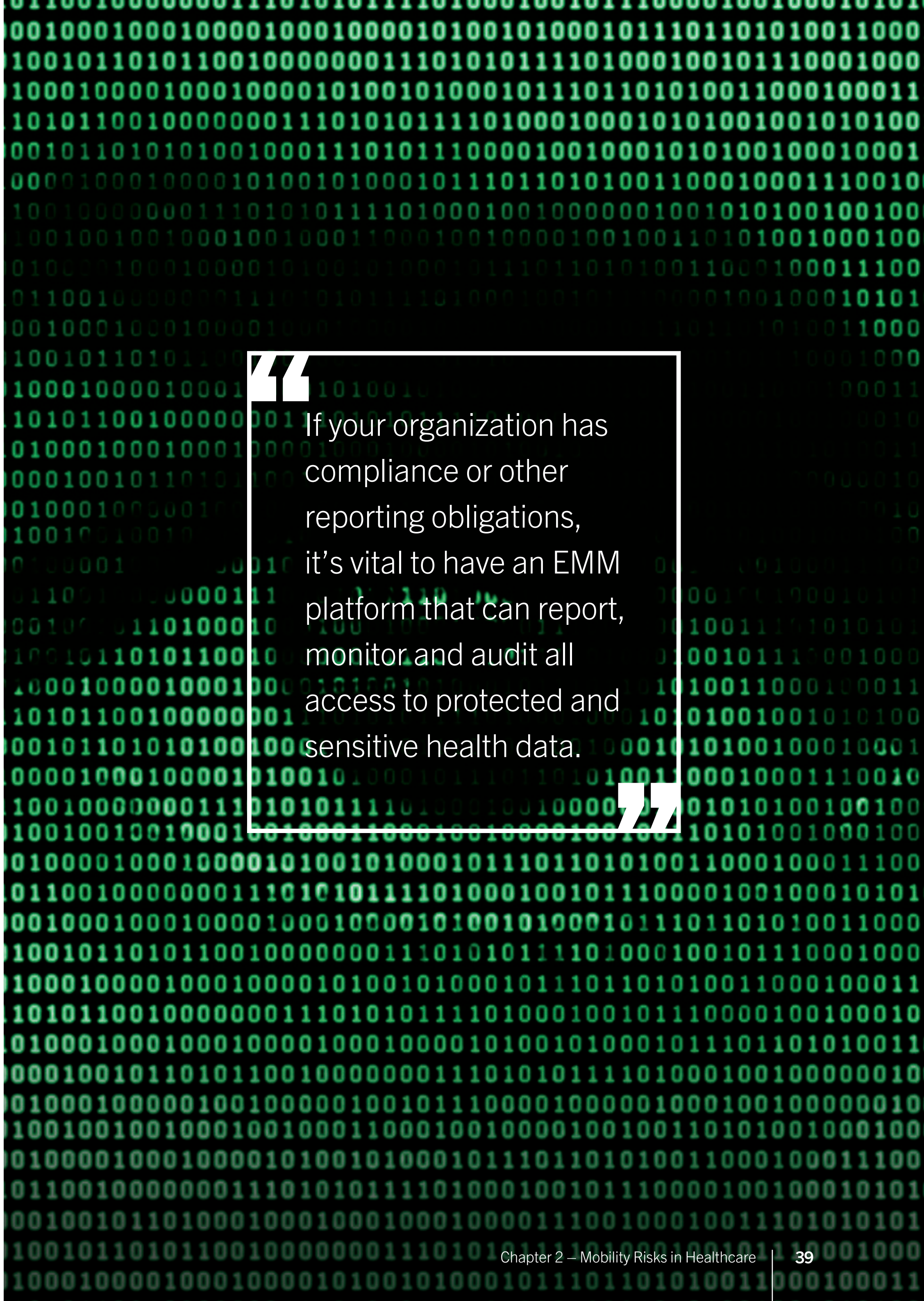
67% of healthcare organizations admit difficulty keeping up with current and emerging mobile security threats.

Source: BlackBerry Mobility Risk Tolerance Survey, Sept. 2014

Other issues are pertinent as well. For instance, does the EMM technology rely on the native device platform? Does it effectively protect data at rest? What about data in transit?

Securing a mobile environment is very different from securing fixed IT assets. Mobile security poses a whole new set of challenges for healthcare organizations, and protecting data requires careful planning and execution. Mapping out your mobile deployment and understanding the attack vectors is the first step towards developing a solid EMM strategy that enables maximum productivity without compromising on security.

Alex Manea is the Director of BlackBerry Security and has been securing mobile platforms for over nine years. He is a Certified Software Security Lifecycle Professional and has an Honors degree in Systems Design Engineering.



“If your organization has compliance or other reporting obligations, it's vital to have an EMM platform that can report, monitor and audit all access to protected and sensitive health data.”

Enabling New Business Functionality Through Secure File Sharing

By Tim Choi, Vice President Product Management, BlackBerry

Cloud storage and collaboration services have made it relatively easy for consumers and businesses to share files and documents online. A growing number of organizations have begun taking advantage of these platforms to access, synchronize, share and manage business information both inside and outside the traditional enterprise perimeter. In an October 2014 report, analyst firm *IDC* estimated that the file synchronization and sharing market would grow at a steady 23.1 percent rate to $2.3 billion by 2018, driven largely by the continuing shift to cloud computing and the growing use of mobile technologies in enterprises.

In the healthcare context, such services can play a vital role in improving patient care, enabling telemedicine and providing universal access to patient data. For instance, cloud storage and sharing services can help expedite patient treatment and diagnosis by giving doctors and other healthcare professionals a secure way to collaborate with each other on patient care. Similarly, they give clinicians and caregivers a way to synchronize and share patient files across their delivery network and with providers of ancillary services. Cloud storage and collaboration tools in essence provide mobile healthcare workers with anywhere, anytime access to critical data.

For hospitals that still rely on outdated paper-based systems such as faxes and printers to share information, the twin trends of cloud collaboration and mobility promise to drive down costs and improve productivity in dramatic fashion.

Security Considerations

Security however, should be a crucial consideration, especially for healthcare organizations. Many file sync and share services are consumer oriented with the ability to sync, share, and collaboration, but do not offer all the security controls mandated by HIPAA and other healthcare regulations.

It is not unusual for employees to use consumer-grade file sharing services to share and collaborate on documents outside of IT's purview. Such sharing can lead to unauthorized data access, data loss and leakage of critical healthcare information. Because many consumer-grade file sharing services lack critical permission policies and monitoring and auditing functions, there's little control and visibility over file access and use. Organizations have no way to assign accountability for changes to the underlying data. Neither do they have the ability to track or monitor compliance violations.

ONLY 28% OF HEALTHCARE ORGANIZATIONS ARE VERY CONFIDENT THAT DATA ASSETS ARE FULLY PROTECTED FROM UNAUTHORIZED ACCESS VIA MOBILE DEVICES.

Source: BlackBerry Mobility Risk Tolerance Survey, Sept. 2014

How Healthcare Can Use Secure File Sharing

There are several use cases for secure file sharing in a healthcare setting:

Sharing patient information

A clinician may want to consult with a specialist on the best options for treating a patient and need to forward the patient's records, medication details, previous illness history, blood work, CT scans and other details. A secure shared workspace can enable this process in a relatively straightforward manner and with none of the risk or manual work involved with paper-based processes like faxing or emailing attachments. A shared workspace allows a venue for streamlined one-time collaboration, regardless of access device type or access location, including between institutions.

Sharing healthcare research data

Medical research teams at universities and hospitals are heavily dependent on patient data such as test results, drug responses and case histories for their research. The data is often shared among multiple people and organizations. The files can also be large – it's common for 10 GB files to be transferred. Because of the highly sensitive nature of the information, organizations can easily fall out of compliance with HIPAA and other regulatory requirements, if they are not careful about the manner in which they enable access to the data.

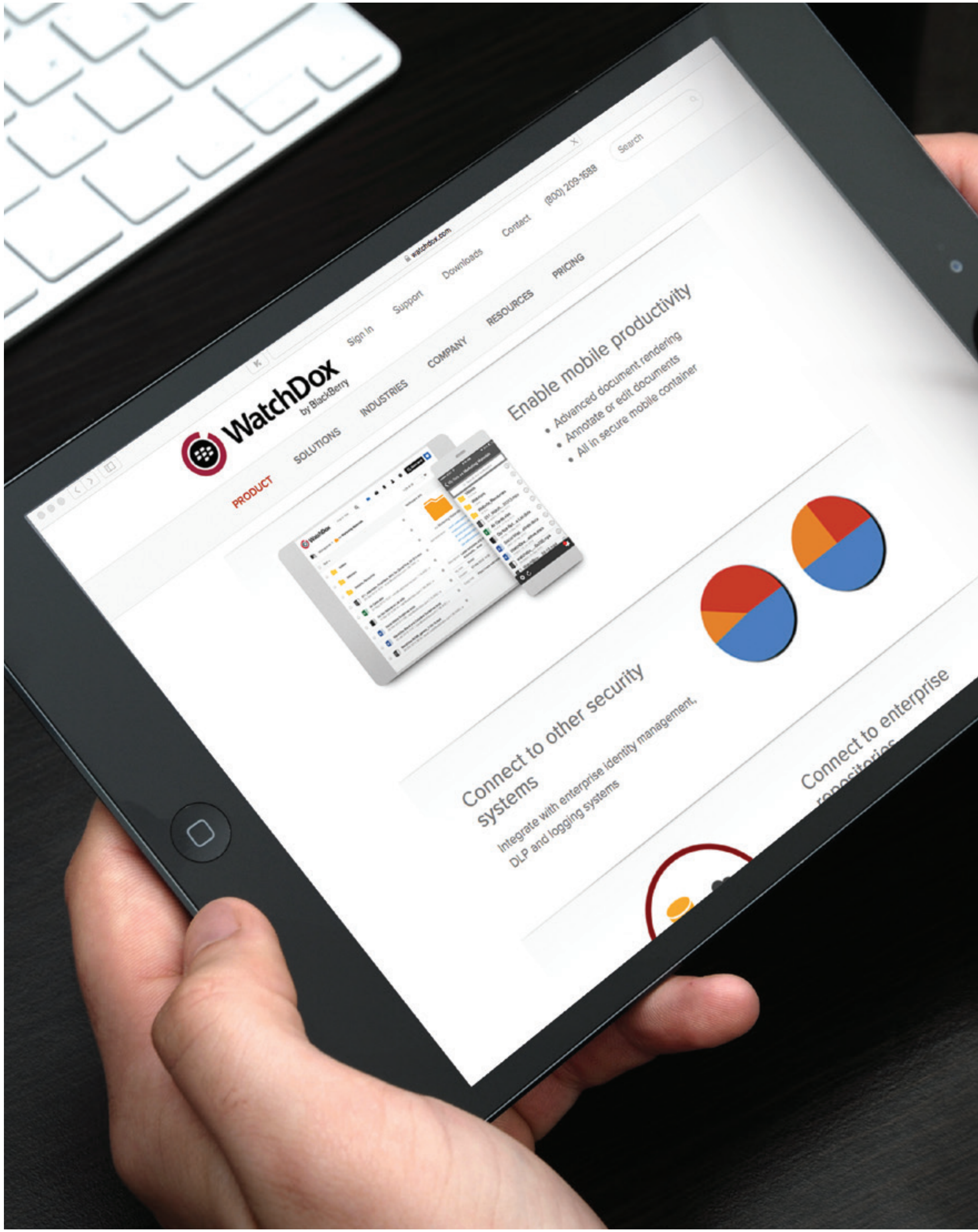
Access control and authentication functions are crucial to have in place, to ensure that only properly authorized people from the research group have access to the data. It allows administrators to quickly revoke access to a researcher that might leave the organization in the middle of a project.

Secure Collaboration with WatchDox® by BlackBerry®

WatchDox by BlackBerry provides a way for healthcare organizations to enable file sharing and collaboration in a manner that is consistent with the security and privacy requirements of regulations such as HIPAA, the HITECH Act and the Emergency Medical Treatment and Active Labor Act (EMTALA). It enables healthcare workers to access, share and manage files with the same ease-of-use as consumer-oriented cloud collaboration services but with the enterprise grade security required to protect health data and adhere to compliance standards.

ONLY 53% OF HEALTHCARE PROVIDERS CONSIDER THEMSELVES READY TO DEFEND AGAINST A CYBER-ATTACK.

Source: KPMG Healthcare Cybersecurity Survey, 2015


watchdox.com
WatchDox by BlackBerry
Sign In
Support
Downloads
Contact
(800) 209-1588
Search
PRODUCT
SOLUTIONS
INDUSTRIES
COMPANY
RESOURCES
PRICING
Enable mobile productivity
• Advanced document rendering
• Annotate or edit documents
• All in secure mobile container
Connect to other security systems
Integrate with enterprise identity management,
DLP and logging systems
Connect to enterprise repositories

WatchDox by BlackBerry is unique in that the document encryption and controls stay with the file even when it is shared on unmanaged end-points. This means that users and administrators can track and audit who is accessing files – an important HIPAA requirement. WatchDox can also revoke access or remotely delete these files. WatchDox by BlackBerry allows users to access documents from PC and Mac desktops, tablets, and smartphones, giving employees the flexibility to work across locations and be productive no matter where they are. It is available both as a cloud service and as an on-premise solution to meet all IT environment requirements.

Enabling Business Functionality through Security

The security controls in WatchDox by BlackBerry are implemented in a manner as to enable a high degree of security without hindering business functionality and productivity. For example, sensitive patient and health data is always encrypted while the data is at rest, in transit or in use using strong cryptography certified by the U.S. Government's FIPS 140-2 standard. At the same time the encryption does not hinder ordinary business use. WatchDox by BlackBerry enables users with a full suite of collaboration tools such as the ability to edit, annotate and share their files easily.

WatchDox lets users and administrators track and audit who is accessing files – an important HIPAA requirement.

As owners and managers of protected data, healthcare organizations can also benefit from technologies that allow them to exert rights management over critical data. WatchDox by BlackBerry implements several workspace and document-level controls that extend this precise capability. For example, it supports permission to download or restrict to online view, permission to print, permission to forward or to edit, copy and file. WatchDox also uses dynamic watermarks, displaying the reader's e-mail address and other identifying information, to protect against unauthorized screen captures. It lets administrators revoke or withdraw permissions when an employee has left the organization or no longer has access rights to business data.

Enabling Mobile Collaboration

A large U.S.-based provider of hospital-based clinical outsourcing services is currently using WatchDox by BlackBerry to secure sensitive documents, including EHR for the entire enterprise. It has deployed WatchDox as an on-premise virtual appliance in the data center to control and manage the manner in which the data is accessed, used and shared by authorized users. The solution has enabled everyone from board members to physicians at the organization to securely exchange, coordinate and collaborate on files containing sensitive data while ensuring proper access controls. Using WatchDox by BlackBerry, administrators at the outsourcing service can control how the data is edited, copied or printed to prevent unauthorized use.

In the healthcare industry, the efficient delivery of timely and accurate information can literally make the difference between an individual's life and death. Mobile and cloud collaboration technologies like WatchDox by BlackBerry offer organizations a secure alternative to paper-based manual processes for sharing clinical and other data. Organizations that fail to take advantage of such tools are exposing themselves needlessly to compliance violations, increased cost and security risks while missing out on an opportunity to improve patient care and management.

As Vice President of Product Management at BlackBerry, Tim Choi leads global product management teams overseeing WatchDox by BlackBerry, which provides secure and productive file sharing, as well as BlackBerry Virtual SIM Services, which powers WorkLife by BlackBerry and ManyMe by BlackBerry. Tim joined BlackBerry through the acquisition of WatchDox, where he defined the roadmap, product messaging and training.

Leading US Hospital-Based Clinical Outsourcing Firm Adopts WatchDox for Mobile Collaboration

Clinical outsourcing providers help hospitals and healthcare organizations with staffing resources during peak seasons and emergency events.

Like other healthcare organizations, the company is under the scrutiny of HIPAA and HITECH when dealing with patient information. Like many other enterprise organizations, the company was in search of ways to modernize their business processes for their mobile workforce. The nature of the business requires employees to constantly move between hospital sites and systems, which exacerbates the challenge of tracking patient information and keeping documents consistent.

Ultimately, the company found a single, comprehensive solution in WatchDox that addressed both their compliance as well as their usability needs.

Customer

- Among the largest providers of hospital-based clinical outsourcing in the United States.
- Delivers services in multiple departments, including Anesthesia, Hospital and Emergency Medicine.
- Corporate headquarters located in Knoxville, Tennessee (US).

Solution

- Deployed WatchDox as an on-premise virtual appliance to allow full control of information.
- Administratively configurable policies to control sensitive data by default.
- Secure enterprise drop box alternative, mobile productivity and external file sharing solutions across the organization.

Goals

- Secure documents including electronic health records (EHR) for the entire organization.
- Support mobile devices used by clinicians, specifically iPads.
- Securely exchange, coordinate and collaborate on files. Control file access, edit, copy and print privileges to prevent unauthorized use.
- Fulfill stringent security mechanisms required by HIPAA & EMTALA.

Benefits

- Comprehensive security architecture, with fully encrypted and tracked information fulfilling HIPAA and EMTALA compliance requirements.
- Peace of mind that information is not leaked, putting the business and company reputation at risk.

> With WatchDox, we now have peace of mind, since our sensitive data is always secure, no matter the device on which it's accessed.
>
> **Mark Cantley, Systems Engineering**

The Solution:

The company decided to deploy WatchDox as on-premise virtual appliance, located in the central data center. This allowed them to have full control to dictate and manage where the data was physically located.

Another benefit that the company derived from WatchDox is that administrators can configure policies to control and track sensitive data by default, with features such as domain and group permissions.

There are three key use cases of WatchDox at the company:

1. **Secure "Dropbox":** WatchDox offers a secure, enterprise-ready alternative to consumer file sync solutions, such as Dropbox, for all users to share and access information on their various devices. WatchDox gives users the expected functionality, with additional consideration for organizational administration and security mechanisms built into the system.
2. **Secure Mobile Productivity:** When it comes to consistent security, it is critical to integrate productivity tools because once content leaves the system all tracking and security mechanisms are lost. Thus, the integrated annotation capabilities that WatchDox offers is a critical aspect of truly secure collaboration. Integrated annotations allow physicians to make notes and communicate information consistently and effectively through notes, highlights and drawings – many of which may be in regards to sensitive patient information.
3. **Secure External Sharing:** As outsourced contractors to hospitals and healthcare organizations, company employees are consistently regarded as "external" users to the organizations that they serve. However, to effectively do their jobs, they must access the same patient information that "internal" hospital staff does in order to provide proper care. Thus, employees must be accountable to fulfill the most stringent policies and requirements expected of even their most demanding customer organizations. With WatchDox as their corporate standard for document management, there is no question as to who is accessing their documents, where from, what device and how they are used.

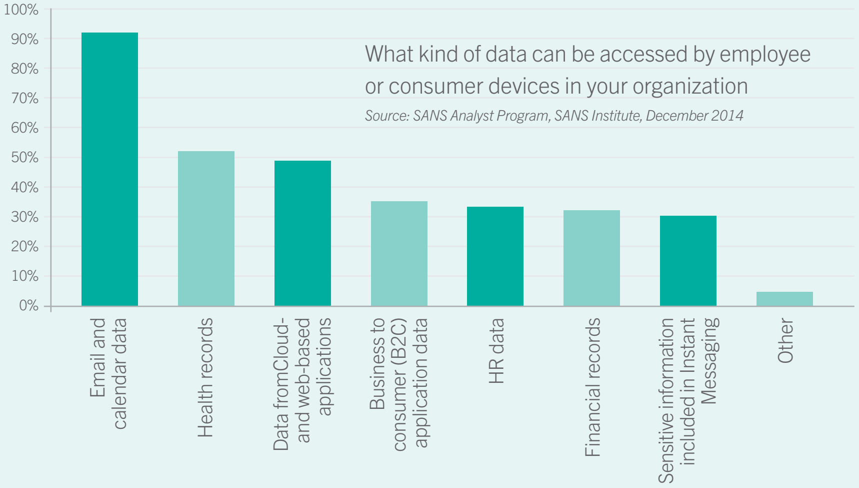
16% OF HEALTHCARE ORGANIZATIONS SAID THEY CANNOT DETECT IN REAL-TIME IF THEIR SYSTEMS ARE COMPROMISED.

Source: KPMG Global Mobile Banking Report, July 2015

The Benefits:

With WatchDox, the company can rest assured that all of their corporate documents stored within the system comply with information security regulations, such as HIPAA and EMTALA, on every device. Additional mechanisms and tools are not required to encrypt and control documents that potentially contain patient data – all information is equally accounted for with the utmost levels of security. Likewise, audit logs and customizable reports tracking file activity can be easily accessed and exported when regulators and upper management require reviews. Mark Cantley, of the Systems Engineering Group at the company shares, "With WatchDox, we now have peace of mind, since our sensitive data is always secure, no matter the device on which it's accessed."

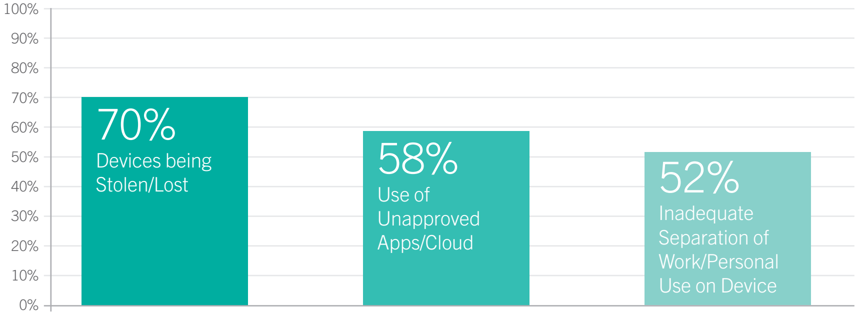
Healthcare Organizations Need to Secure Their Data



What kind of data can be accessed by employee or consumer devices in your organization

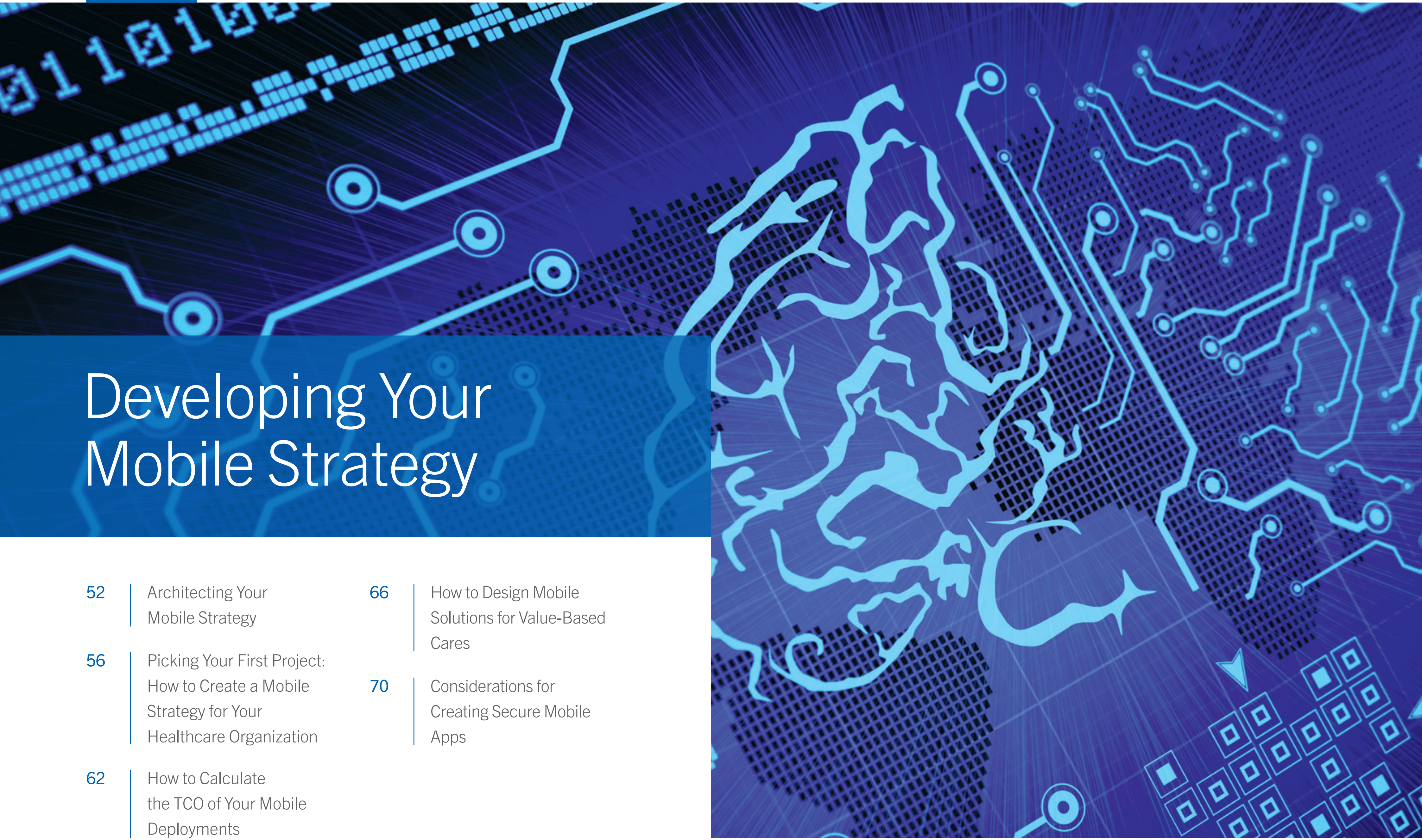
Source: SANS Analyst Program, SANS Institute, December 2014

Key Enterprise Risks for Healthcare Organizations



Source: SANS Analyst Program, SANS Institute, December 2014

Chapter 3



Developing Your Mobile Strategy

Architecting Your Healthcare Infrastructure

By Mark Wilson, Chief Evangelist, BlackBerry

Data is the blood that drives your business, but your technology infrastructure is the veins and arteries and organs that keep the blood pulsing through your company, keeping all the essential parts connected. Your mobile devices, smartphones, tablets, embedded Internet-connected systems, software and networking equipment are key components of that overall infrastructure. These components ensure that your healthcare providers have the information they need at their fingertips, right when they need it.

Creating a mobility strategy is more than just adding smartphones or tablets to your corporate network. Your mobile strategy should involve matching state-of-the-art mobile hardware and application software with the right mix of policies, procedures, and practices that blend mobile technology into a healthcare business environment. In addition to the requisite network hardware, business and mobile applications, and devices, you need to implement Enterprise Mobility Management (EMM) software that manages devices across multiple operating systems, so it can grow as your environment does. At the core, however, is ensuring your mobile strategy meets the needs of your organization to improve patient care, increase efficiency of staff, maximize satisfaction and ultimately deliver better patient outcomes.

> “Creating a mobile device strategy is more than just adding smartphones or tablets to your corporate network.”

> “A reference architecture design that puts the key components in place can save a healthcare facility a lot of time and money, and eliminate gotchas that might lead to lost productivity, compliance failure and compromised security.”

Using a Reference Architecture

One tool that can help create your mobile strategy is a reference architecture. A reference architecture helps to outline the possible use cases that will provide value to your organization, and identifies the hardware and software vendors with tested and certified products that meet the exacting demands for a healthcare organization. For the healthcare industry, it is important to meet compliance rules and regulations that are specific to your location, and to show how mobile devices are connected and managed within your environment. These devices can be smartphones, tablets, or embedded devices such as sensors that connect medical equipment to the Internet so that doctors or first responders can monitor patients remotely or in transit.

BlackBerry has a well-defined reference architecture for the healthcare industry, using proven, best-of-breed hardware and software from leading technology vendors. It includes use cases and solutions across the full continuum of care – from remote clinics to home environments to hospitals.

The BlackBerry Reference Architecture for Healthcare

Let's take a look at each of the use cases listed in the BlackBerry healthcare reference architecture.

In a facility that uses multiple mobile computing platforms, cross-platform EMM software is configured to communicate with iOS, Android, BlackBerry and Windows Phone devices, managing IT policies for each platform. The EMM software uses a containerization approach to ensure the data is protected, regardless of which platform it resides on, and the management capabilities ensure that auditing, archiving and security are in place.

Mobilizing tools to enable clinical collaboration ensures that healthcare providers have the most current data and are able to collaborate with each other, regardless of where the providers are located and which type of device they are using to access the data. Improved patient care, lower costs and protection of the patient's privacy result when providers have everything they need at their fingertips.

Hospital staff coordination ensures that everyone within the medical center, be they operating room personnel, clinicians, technicians, hospital staff and management, transportation staff and housekeepers are able to ensure that the patients get the best care possible with the least amount of inconvenience. Efficient staff coordination results in reduced expenses, higher satisfaction for staff and higher levels of patient service.

The ability to receive alerts, alarms and notifications on mobile devices, and using smart systems to route the alerts, means that clinicians are only receiving notifications for information and tasks that apply to them. This enables them to be more efficient and reduces "alarm fatigue" – a condition that occurs when the volume of irrelevant alerts grows too overwhelming. It also means less overhead noise and alarms in patient rooms, which means a quieter and more peaceful environment where patients can recover.

In a remote clinic, healthcare professionals can access necessary patient records and other medical services using a single sign-on and secure file sharing from any enabled devices. Essentially, this creates a mobile clinic, providing healthcare professionals the same level of access if the patient is in the hospital, a remote clinic, or even in their home.

In a mHealth environment, sensors can collect biometric data from a variety of devices, such as those monitoring a patient's temperature, blood pressure, pulse, weight, and blood sugar. The Bluetooth technology can then transmit the data to a mobile device that connects to the network securely, providing real-time and trending data to the monitoring care givers. Patients and care providers can receive scheduled reminders and alerts.

More and more patients are using Web apps and portals to help manage their own care. Some innovative healthcare facilities are taking this patient communications to a new level beyond just web portals. Secure messaging between providers and patients, screen sharing, video conference and secure file sharing represents the next level in including the patient in their healthcare services.

Therapists, traveling nurses and other healthcare professionals providing home care not only need access to the patients' records using a very secure data transmission connection, but they also benefit from geolocation services that help them reach their charges most efficiently and quickly. Once at a patient's home, the provider can use their mobile device for video conferencing, secure messaging, creating or accessing a patient's care plan, scheduling or virtually any service that can be provided within a healthcare facility.

First responders benefit from mobile solutions by having the tools necessary to provide high-quality care in conjunction with the healthcare professionals at the hospital wherever the first responders happen to be. With secure messaging, file sharing, video conferencing and voice calls, along with using mobile devices along with remote medical devices such as a mobile ECG device, first responders at the scene of an emergency and in transit have greater access to healthcare professionals and medical device capabilities than ever before.

The bottom line is creating a safe and secure environment for healthcare professionals to access data they need anywhere, at any time, on any device, so they can best care for their patients. A mobile strategy designed with these use cases in mind can make any facility or medical professional more efficient and enable them to provide higher quality patient care.

In the next sections of this chapter of this guide, we'll explore how you can evaluate each use case for your healthcare facility and then rank your use cases by the highest value and greatest feasibility. This ranking can help you identify which projects should be your highest priorities. This prioritization of projects will also help you with budgeting and personnel planning in the long term as you grow your environment and become a true Smart Hospital.

As Chief Evangelist at BlackBerry, Mark Wilson is responsible for delivering the BlackBerry message through thought leadership and other opportunities that promote the brand. Mark leads a cross-functional team at BlackBerry dedicated to helping BlackBerry customers in healthcare drive tangible benefits from their mobile deployments.

Picking Your First Project: How to Create a Mobile Strategy for Your Healthcare Organization

By Jeff Holleran, Vice President Corporate Strategy, BlackBerry

The vast array of potential mobile strategy projects in healthcare can be overwhelming. The combination of personal and company-owned devices requires effective organization and management. Connecting medical staff with first responders and home providers is essential, but is that a higher priority than implementing a program that connects medical devices to the nurses' stations? Is your mobile program in compliance with federal regulations to protect confidential data? Do you have the foundational Enterprise Mobility Management (EMM) software in place on which to build an effective project? You can compare the building of a mobile strategy to a game of Tetris – lots of moving parts that need to fit together in a coherent and organized manner.

One size fits none when determining how and where to start an enterprise mobility project. Every healthcare organization has different risks; therefore, every implementation will have its own priority projects.

Identifying a Project

Communication and collaboration using mobile devices is changing how we deliver healthcare and adding layers of complexity to the corporate network infrastructure. As the network framework grows, much of it is no longer in the physical control of the corporate IT department. Today's network perimeter – that line where your network ends and you connect to the Internet – stretches into personal and mobile devices, the cloud, and corporate networks of business associates as defined by regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the Personal Health Information Protection Act (PHIPA) in Canada. Protecting patient data, regardless of where it resides, is a top priority of IT decision makers and a driver of your risk profile.

Implementing an EMM system is an essential first step for any overall mobile project. This framework provides organizations with the ability to connect to devices, such as smartphones and tablets, and manage services and content on them. This could include anything from messaging to applications to data containers to keep personal and work data separate.

One of the most difficult issues IT and security staff face today is managing confidential and protected patient data and the user's personal data on mobile devices. Confidentiality and compliance with federal regulations are paramount regardless of whether a medical center has a Bring Your Own Device (BYOD) policy, Choose Your Own Device (CYOD), Corporate Owned, Personally Enabled (COPE) or Corporate Owned, Business Only (COBO) environment.

Creating Use Cases and Projects

Let's look at some of the possible use cases a healthcare organization may choose to mobilize. Your initial project could be strategic or tactical. Often a pilot project will help you evaluate the feasibility, time, cost, and impact that the technology will have on your workflow and IT infrastructure. Here are some potential initial projects:

1. Expand the reach of a local or regional facility by letting remote physicians and clinic staff connect with mobile devices. Medical staff can securely share documents on any mobile device, ensuring that patient privacy and confidentiality are maintained.
2. Provide home care workers with mobile devices to connect to the corporate network and communicate directly with the medical staff. Home care workers can automatically send alerts from medical devices, such as sensors tracking a patient's vital signs, to the hospital so that nurses, therapists, technicians, or other medical personnel will know if the home care provider needs to act.
3. Enable mobile clinical collaboration between doctors, nurses, therapists, technicians, and other members of the medical team so they can work together regardless of where they or the patient are located.
4. Share all types of medical files on mobile devices, including videos, X-rays, and other medical imaging results.

The opportunities for using mobile technology to enhance healthcare operations don't stop here. There are many opportunities to mobilize your workflow and processes to improve patient care and the efficiency of your staff. But how do you choose which project to begin with? In order to help you choose where to start, it's important to take a step back and look at the bigger picture.

> "Doctors, nurses, therapists, and technicians can now all work together regardless of where the patient or client is located."

Using a Value Feasibility Matrix

The goal for any major IT project should ultimately be to solve a key business problem. What are your employees saying they need? What complaints are coming from your customers? You'll want to talk to your users to get a full view of the challenges your mobility project will need to solve.

Once you have a list from your end users of challenges to solve, take a look at your risk profile. Where is the organization vulnerable? Your chief information security officer and your chief risk officer need to be part of the team that determines where you should start, based on the organization's overall corporate risk analysis. This is an important step that should be undertaken before identifying which project to start on, because the risk analysis results will provide vital information about which projects are most needed.

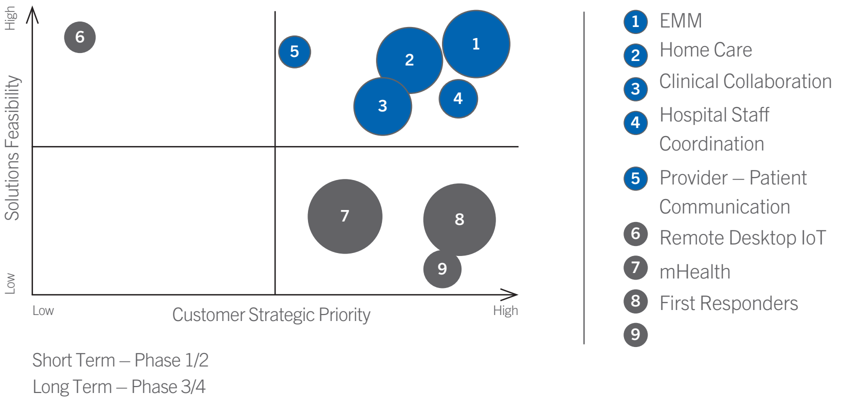
> While there might not be any obvious first choices for mobile projects, there are a lot of good choices.

The next step is to create a matrix of possible projects to consider, to evaluate their overall value to the company and their feasibility in order to meet the long-term goals you identified in the previous step.

A sample value feasibility matrix is shown here. The Value axis should consider such aspects as how well the project satisfies your business needs for improving patient experience, regulatory compliance, return on investment, and lowering corporate risk. Which of these are your most strategic priorities? The Feasibility axis addresses hard costs for hardware and software, staffing, personnel training, and soft costs for systems integration, consulting, and unexpected or unknown expenses.

Other items which may be considered include the immediate need for preventing and resolving data breaches or vulnerability remediation, corporate priorities, and what might be called the squeaky wheel effect.

Value – Feasibility Matrix



This latter component might include a pet project, a complaining department head, or a response to negative publicity. One must be very careful about placing too much emphasis on these items; they may or may not align with your long-term strategic goals.

The value feasibility matrix will help you identify key pain points in your overall healthcare reference architecture and where your need for mobility may be greatest.

Deploying a Mobile Project

After you identify a project, make sure that you have buy-in from senior management, IT, risk teams, clinical decision makers, and your end users. Your budget should include not only the cost of the software and requisite hardware, but also the cost of configuring the software and additional consulting and training.

First year costs likely will be higher because of non-recurring costs, such as software configuration, consulting, and possible hardware. However, training costs should be budgeted yearly to address turnover or project growth. In the second year and subsequent years, one standard recommendation is to budget one-quarter of the software cost for software support with an equal amount for maintenance and training. These estimates will vary based on each implementation.

You should build in periodic reviews of each operational component of your mobility program to ensure that it continues to be relevant and effective. As part of the planning process, create some basic metrics that can be used to measure the effectiveness of the program.

Measuring the Results

After you have implemented your program, measure the implementation's actual results against the expected or anticipated results. Are the results of the program consistent with the results that you expected? And more importantly, is your staff happy with the solution? Are they using it or are they finding workarounds to get around it? Have you solved the key business challenges you identified in the first step of the process?

As previously mentioned, no universal first project for healthcare mobility exists; even installing an EMM foundation on which to build your mobile environment might be a secondary or tertiary priority. Perhaps your fundamental need is collaboration and messaging. It might be something as basic as mobilizing a dashboard to give clinicians and staff greater visibility into patient flow in your hospital. But while there might not be any obvious first choices for mobile projects, there are a lot of good choices. Don't wait to start figuring out what the best choice may be for your organization.

Jeff Holleran is the Vice President, Corporate Strategy at BlackBerry and leads the Corporate Strategy team responsible for identifying and operationalizing global strategic opportunities to enhance BlackBerry's portfolio.

How to Calculate the TCO of Your Mobile Deployments

By Mihir Andrei Mukherjee, Director, Global Sales Initiatives, BlackBerry

At a high level, there are essentially two ways to think about the business value derived from an Enterprise Mobility Management (EMM) suite, or from any technology for that matter. The first is the value derived in terms of business benefits: improved productivity, better operational efficiencies, enhanced resource utilization, reduced risk of data breaches and similar other tangible or strategic benefits. The second is the cost of delivering that value – i.e., the total cost of ownership (TCO), which is an examination of the cost-effectiveness of using a particular technology. At BlackBerry, we encourage our customers to evaluate both aspects thoroughly when doing a value analysis for EMM.

Multi-faceted, Multi-dimensional

When you look at TCO, there are multiple elements that need to go into the model beyond the technology licensing costs. What you pay to buy and deploy an EMM technology has significant bearing on the overall TCO. But there are also the costs involved in maintaining the technology on an ongoing basis and what you would need to pay to ensure an adequate level of support for all your users.

We think of TCO as having four distinct components to it: the hardware cost, the software license fees that you pay the vendors, the support services costs, and maintenance and upgrade fees for the hardware and software as needed. Any TCO analysis that does not include all four components is incomplete at best.

Making Apples-to-Apples Comparisons

When comparing TCO across multiple vendors and technology platforms, resist the temptation to look just at the hardware and software license costs. While they are often the easiest to compare, you must make sure that you do an apples-to-apples comparison across feature sets and technology capabilities. An EMM suite that comes in with a lower initial price tag may not have all the features offered by a seemingly pricier product. Your cost analysis should compare similar products, or as close to similar feature sets as vendor differences permit.

Service, support, and maintenance costs have a big impact on TCO. These costs can vary significantly from vendor to vendor based on factors like pricing tiers, number of users, number of devices supported, and the desired level of EMM functionality. Making these comparisons can be tricky. Vendors can have different pricing structures for on-premise implementations versus cloud deployments. Some vendors might have an annual subscription model, while others may price their technology on a perpetual, quarterly or monthly basis. Some, like BlackBerry, include maintenance and support costs in the annual subscription fee. Other vendors break these costs down separately.

Understanding the Differences

Vendor tiers that categorize different service levels are not always directly comparable. What one vendor might offer as part of their basic support package is something that might only be available in a premium support and service package with another vendor. Sometimes, it's worth paying a higher upfront price for an EMM suite because it is more easily integrated and interoperable with multiple technology platforms, instead of a product where you would need to pay separately for software and services to implement that integration. Volume discounts and special pricing based on existing relationships can also have an impact on TCO.

It is a good idea to examine each component of the TCO model and not get fixated on technology costs alone but rather the cost of owning that technology over a specific period of time. It's important to note that contract duration plays a role in TCO as the annual components could add up.

> When comparing TCO between vendors, make sure you are doing a true apples-to-apples comparison for features, functionality and deployment methods across all elements of a solution, not just licensing cost.

> It can be worth paying a higher upfront price for an EMM suite that is more easily managed, integrated and interoperable with multiple technology platforms.

Estimating Business Value

In terms of business value, the benefits that an organization might derive from a technology depend on a variety of factors. Benefits realized can vary based on process maturity, staff resource availability, existing technology infrastructure, successful change management and willingness to invest in necessary upgrades and enhancements.

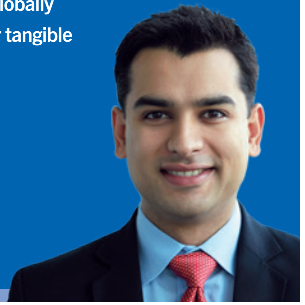
For example, a healthcare organization with an ancient technology infrastructure will likely have a harder time realizing the full benefits of enterprise mobility than an organization that is better prepared to take advantage of it in terms of interoperability with existing systems. Similarly, a business that has employees with advanced technology skills might access mobility benefits more quickly – and more of them – than an organization whose staff is still only coming up to speed in those areas. These nuances must be taken into consideration when creating a business case. What worked in other companies or in your prior experience may not deliver the same value due to a new set of variables that must be accounted for.

The Constant Factors

Even so, there are ways to derive relatively accurate estimates of business benefits from a technology implementation by looking at some of the factors that do not change. Within healthcare, the hourly rate for a nurse or the cost associated with staff training is roughly the same across organizations. Similarly, the recurring cost savings that might result from reducing staff turnover, or by improving nurse scheduling and dispatching is unlikely to vary much across organizations.

The key point here is that, while the magnitude of the business benefit itself might vary from organization to organization based on factors and nuances mentioned above, the areas of value remain consistent for the industry. Regardless of where your organization might be in terms of its readiness to exploit a technology, there are ways to make a reasonably accurate prediction of the business value you will most likely derive from it. To help our customers predict this business value, BlackBerry has developed a set of TCO calculators and business value calculators for some very specific mobility use cases within the healthcare sector. Later on in this book, we will show you how to use these calculators within your specific environment to generate both conservative and reasonable estimates of your ownership costs and the recurring benefits from your enterprise mobility investments.

Mihir Andrei Mukherjee is Director of Global Sales Initiatives at BlackBerry and is a thought leader responsible for working with customers to help identify, quantify and realize their business and strategic goals through BlackBerry technologies. Mihir is an expert on value selling and has worked with business leaders globally to deliver tangible results.



How to Design Mobile Solutions for Value-Based Care

By Claudius Metze, Senior Solution Architect, SAP SE

There is little disagreement that mobile solutions are poised to have a dramatic impact on the delivery of healthcare services in the years ahead. For the healthcare industry, the coming mobile health revolution holds the promise of reduced errors, better collaboration, increased efficiencies and lowered costs. But this doesn't mean that every mobility strategy implemented will be successful. Without proper planning, projects are very likely to fail. A key component of successful mobility strategies is a design that seeks to solve specific real-world challenges and address clearly identifiable process inefficiencies. At the same time, the solution must ensure the security of data and comply with privacy guidelines. When these factors are in balance, you are more likely to achieve your mobility goals.

At SAP, we refer to the design and implementation of new technology and processes that respond to specific problems and inefficiencies as *design thinking*. It's a methodology that seeks solutions and efficiencies that correspond directly to clearly identified problems and processes. It requires you to first understand the actual problem that needs to be solved, so you're not making assumptions about the impact of a new process or being wowed by new technology. The goal is to make decisions in an environment void of preconceived ideas and biases. Design thinking also forces you to first understand on a step-by-step basis current processes and workflows. Often, design thinking requires user shadowing so that you can see what workarounds the users engage in on a regular basis. Sometimes these are things the users would never articulate and may not even be aware they're doing.

> The Design Thinking methodology forces you to understand the actual problem, including current processes, workflows AND user workarounds.

For example, a healthcare organization may want to give clinicians mobile access to patient image x-rays and MRIs. Mobilizing the organization's image archiving system will make these files more accessible to staff. But introducing this system will likely also hinder workflow unless it also connects to relevant patient data housed in other systems. A design thinking methodology would uncover this issue before the new mobile-based imaging access system was implemented, because a shadowing exercise would reveal that clinicians have to exit the application to go into other relevant medical record databases to get a complete picture.

Too often, healthcare organizations fail to take this high-level approach to planning out their mobility projects, and the result is that they don't see true business value from these projects. A recent study done at one of the largest and most renowned hospitals in Europe provides an example of a design thinking approach to a mobile strategy. The *14-week study* ❯ conducted at Charité Universitätsmediz in Berlin compared the results of a group of neurologists who were provided with tablet computers to access patient records with a group of neurologists who did not have access to tablets. The study concluded that, as compared to the control setting, neurologists with tablets spent more time in face-to-face consultation with patients. The presence of tablets also resulted in a better workflow as the doctors were able to check records more quickly when they were making rounds and meeting with patients. The study concluded that overall the tablet computers with mobile records enhanced clinical workflow and increased bedside time.

> Tablet-equipped physicians are able to check patient data more quickly and as a result spend more face time with patients.

The Charité Study enabled us to quantify the value of the mobile solution. The study serves as an example of not only the efficiencies mobility solutions can offer, but also the benefits of a design thinking approach. In this situation, there was a singular process that the hospital was attempting to address or improve: neurologists conducting patient rounds. More specifically, this process involved neurologists accessing medical records while checking in on admitted patients. In this case, the solution was a system that included devices in the form of tablets, a secure network and application that allowed the devices to access patients' medical records.

Too often, medical providers see mobility solutions as a take-it-or-leave-it proposition that requires them to make large-scale changes to their IT infrastructure and implement many mobility solutions at once. Providers are generally scared off not just by the daunting and dramatic nature of such change, but also the cost. And for many of those not scared by the cost, there's sometimes an erroneous assumption that throwing money at the issue will guarantee success. In these situations, organizations adopt major changes with the generic goal of being more efficient or technologically advanced. But these advances are not the result of pilot testing, and no processes have been identified that should be improved. The best technology doesn't guarantee success from a value and end user perspective. Technology is not usually the impediment – it's making sure the solution fits the workflow.

Small and clearly defined mobility solutions like the one that was the subject of the Charité study usually present a value proposition that favors adoption. For the costs of the tablets, the secured network and a single application, that provider saw a return in the form of increased efficiency among one of its most valuable resources: neurologists' time. Focusing on a clearly-defined issue also helps to prevent a situation in which mobility solutions are being introduced in an ad hoc and reactionary manner. It's not uncommon for providers to adopt mobility solutions in response to staff who are complaining about a small part of their workflow or who have already downloaded medical applications to their own mobile phones. While situations like this demonstrate the value of mobility solutions, providers must avoid implementing plans that are simply responsive. It's important to have an overall vision of the mobility strategy so that the least number of vendors can be used across the organization, and to make sure that they are interoperable. This reduces complexity and decreases the risk that comes with having multiple connection points across a number of vendors.

In addition to adhering to the fundamentals of design thinking, the Charité study also exemplifies another key component to a successful implementation of a mobility solution: metrics. Even if done on a smaller scale, the implementation of mobility solutions represents a cost for providers. Given that cost, it is imperative that providers devise a system to clearly understand and compute any value that results from mobility solutions. That value doesn't necessarily have to show itself initially in financial benefits. Value could come first in the form of time savings, efficiency and better clinical decisions, but demonstrating that the value exists in each individual setting will be key to the industry-wide rise of mobility solutions.

Claudius Metze is a Senior Solution Architect for SAP SE and is responsible for SAP's clinical portfolio.

Considerations for Creating Secure Mobile Apps

By Brent Thornton, Director Enterprise Solutions, BlackBerry

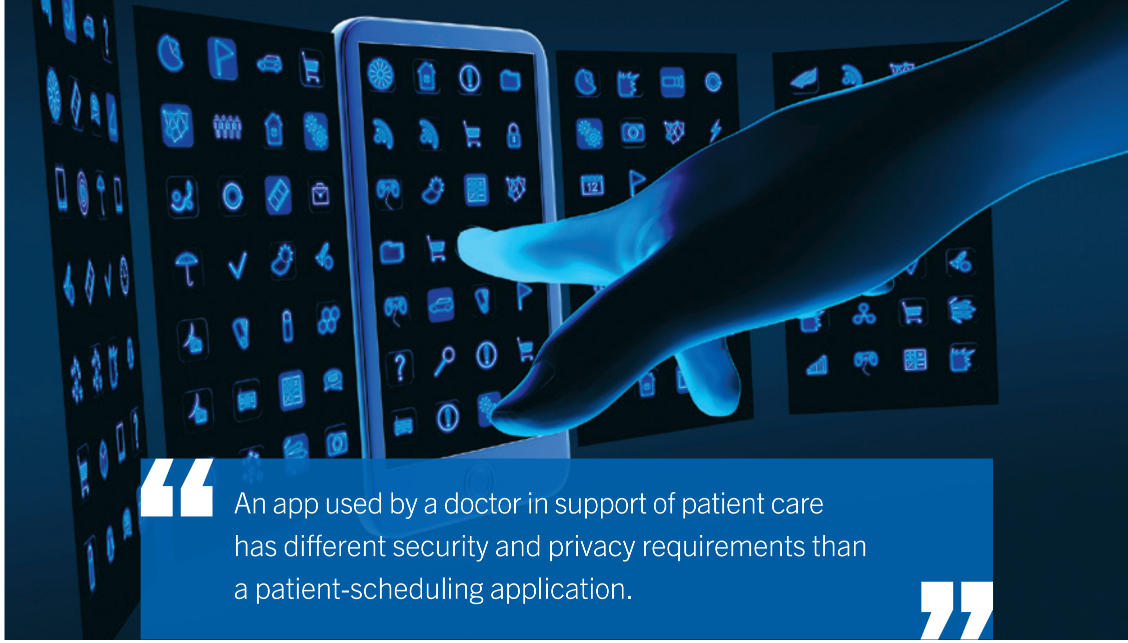
Security needs to be a fundamental consideration when developing and deploying mobile healthcare applications. But it should always be an enabler of new functionality and not a hindrance to it. At many healthcare organizations, enterprise mobility has come to mean a lot more than just having mobile access to email, calendar and contact applications. Increasingly, it is also about bolstering patient care, improving collaboration among physicians, and reducing office visits through the use of mobile monitoring.

Planning for Security

When planning for enterprise mobility in this context, it is important to think in terms of application security. Mobile healthcare applications are vulnerable to software flaws and malware threats in just the same way that desktop and server systems are exposed. Healthcare applications and data running on or accessible via mobile devices are as susceptible to accidental, negligent and malicious exposure as data and applications on any other enterprise system. Practices like device rooting and jail-breaking heighten the risk of malicious actors gaining access to devices containing protected health information (PHI).

Compliance Requirements

Securing mobile applications and data in this environment can be challenging and requires a focus that extends beyond just managing the device itself. Healthcare organizations are governed by regulations like PHIPA, HIPAA, the HITECH Act and EMTALA. The regulations require healthcare organizations to implement specific controls for protecting sensitive patient health information against unauthorized access and use, data leaks and inadvertent or malicious exposure.



> An app used by a doctor in support of patient care has different security and privacy requirements than a patient-scheduling application.

Many of the applications and devices that hospitals and clinicians use in support of patient care and other functions need to be compliant with specific requirements for data security and privacy. One of the biggest factors to consider therefore when developing mobile applications for the healthcare sector is to determine if your application complies with regulatory requirements.

Different Strokes

Remember, not all mobile health applications have the same compliance requirement. An app that is used by a physician in support of patient care will typically have different security and privacy requirements than an application designed for scheduling office visits or for patients to read up on medical conditions. Make sure you understand the specific requirements and other regulatory mandates for your application before setting out to build it.

There are several things you need to do to ensure your application is secure.

Data Encryption

It generally is a good security practice to encrypt data at rest and in transit. In the healthcare context, data encryption is an absolute must. Encryption ensures that sensitive data is protected even in the event of a data breach resulting from a negligent or malicious act.

Considering the proliferating threats against mobile devices, encryption of data at rest or data in transit is the minimum requirement. It's the price of entry to the mobile market place. Make sure your application supports robust encryption of data at all levels.

Beyond Commodity Apps

Commodity
- Email
- Calendars
- Contacts

General Apps
- Web Links
- Dashboards
- Emergency Contact List
- Time Tracking
- Vacation Requests

Unique Apps
- Field Service Input/Ordering
- Asset Tracking

Mobility is Now a Strategic Business Platform

Define User Segmentation
- By Risk Level
- By Policy (i.e. Regulated)

Evaluate Device Inventory
- Current Population
- Allowed By Policy

Identify App Requirements
- Corporate
- Line of Business
- Legal and Regulatory

Level of Investment
- Native vs HTML

Deliver Mobile Platform Solution
- Built In Capability
- 3rd Party Applications
- Web Links
- Custom Applications

Enterprise Mobility & Consumer Mobility

EMM Models
- BYOD – Bring Your Own Device
- COPE – Corporate Owned, Personally Enabled
- CYOD – Choose Your Own Device
- COBO – Corporate Owned, Business Only

Enterprise Mobile Connectivity Application Containerization
- Secure Work Space by BlackBerry® for iOS and Android™
- Samsung KNOX™
- Android™ for Work

MDM/MAM Policy Availability and Enforcement
Application Lifecycle Management

> “HIPAA requires that strong authentication is used to protect patient health information.”

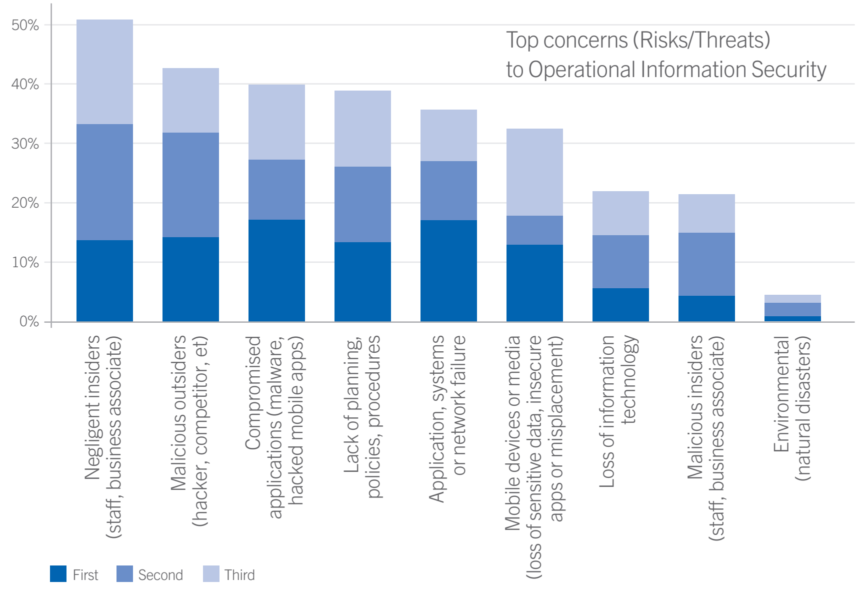
Strong Authentication

HIPAA requires healthcare entities to implement strong access controls to protected health information. Organizations are required to ensure that at all times, only authorized users have access to PHI. When developing a mobile application, you need to ensure support for strong authentication mechanisms. Conventional username and password-based authentication mechanisms are not always sufficient for protecting malicious access to health data. Consider implementing support for multi-factor authentication when designing your application.

Remote Wipe and Reset

Lost or stolen mobile devices pose a huge security and privacy risk especially for regulated industries such as healthcare. More sensitive data is compromised because of a misplaced or stolen device than any other cause. Make sure your application supports capabilities like remote wipe and remote reset. Such functions ensure that sensitive data remains protected in the event that the device itself goes missing.

What do you consider to be the top three risks/threats to your organization’s information security?



Source: IT leaders surveyed by SANS Analyst Program, SANS Institute, December 2014

Mobile Security Concerns

	% 2013	% 2014	% Change
Lack of awareness about security policies	73.2%	73.9%	+0.7%
Insecure/unprotected endpoints	72.5%	73.3%	+0.8%
Loss or stolen devices	82.6%	70.3%	-12.3%
Corrupt, hacked or malicious apps	66.7%	58.2%	-8.5%
Insecure wireless use	47.8%	49.7%	+1.9%
Insecure web browsing	46.4%	38.2%	-8.2%

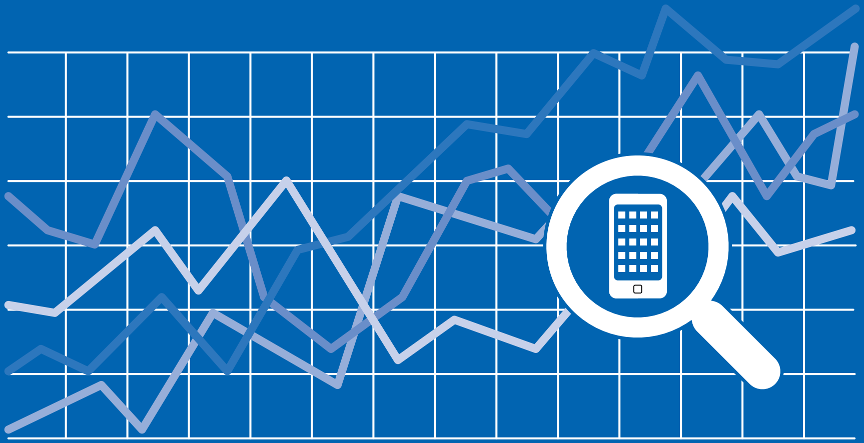
Source: IT leaders surveyed by SANS Analyst Program, SANS Institute, December 2014

Role-Based Access Control

Consider the roles, responsibilities and the authority of those with mobile access to enterprise applications and data. Not everyone will require the same level of access to all data. Some roles require greater access to business apps and data while some roles may require less. Implementing support for role-based access control is critical to ensure sensitive data is not at risk.

Software Updates and Security Patching

Have a strategy for deploying needed software updates and security fixes for your healthcare applications. Unpatched software can give malicious attackers a way to access enterprise data via your mobile device. Modern enterprise mobility management (EMM) technologies support over-the-air updates that make it easy for administrators to deliver updates and fixes across all devices in the enterprise. Ensure that your applications support such capabilities.



Logging and Auditing

When it comes to healthcare apps it's not enough just to implement strong authentication and access controls. You also need to have a way to monitor and log user access and use of PHI. Developers need to implement mechanisms that allow for easy auditability and give administrators a way to determine if protected data has been accessed or modified illegally. This can help detection of threats caused by negligent insiders and may even deter them from ever attempting the malicious act.

Segmenting Personal and Business Data

Considering the widespread use of personally owned devices in the workplace, you need to make sure you have a way to separate protected healthcare data from other content on personally owned systems. Containerization technologies have made it relatively straightforward for developers to securely isolate business use and business data from personal owned data. Consider leveraging such approaches to make it easy for administrators to segment your application and associated data from personal content on end user devices.

Familiarizing yourself with regulatory requirements and knowing your organization's obligations is the best way to ensure the security of your mobile application. BlackBerry can help with your mobile application strategy. Visit *http://developer.blackberry.com* to contact our team.

Brent Thornton is the Director of Enterprise Solutions at BlackBerry and leads a team responsible for helping BlackBerry customers develop in-house mobile applications.

Chapter 4

Cross Platform EMM

BYOD, CYOD, COPE, COBO: Which is Best?

By Billy Ho, Executive Vice President, Enterprise Products and Value Added Solutions, BlackBerry

A funny thing happened on the way to the modern mobile landscape: people started bringing their own smartphones and tablets to the office. It was named Bring Your Own Device (BYOD) and for a few years, BYOD was the hot trend. Employees loved the convenience of having one smartphone capable of both work and play, and even companies who were nervous about security were loath to stand in the way of productivity (not to mention that employees were paying the phone bill). As recently as 2013, market research firm *Gartner* predicted that by 2017 roughly half of all employers would require their employees to supply their own devices. In healthcare, 2014 research by *Spyglass Consulting Group* found that 70 percent of nurses and 96 percent of doctors use personal smartphones while providing patient care.

Today the pendulum is swinging the other way. While BYOD is still popular, organizations are slowly taking back control over business conducted on mobile devices. Why the shift? Lost, stolen, and data-breached personal devices have helped bring about this change. Even employees are pushing back, unwilling to foot the bill for corporate phone use or take on the legal burden of handling company information on their own devices. Businesses can use a variety of strategies available to bring sensitive corporate data back under lock and key while keeping users happy. The main models are recognized: managed BYOD, Corporate Owned, Personally Enabled (COPE) and Corporate Owned, Business Only (COBO).

> “BYOD may increase, not slash, your mobile costs, as helpdesk costs rise and employees balk at covering the bill for work-time phone use.”

With managed BYOD, organizations continue to allow personal devices but require employees to use data management software that shields company information. With COPE devices, businesses issue smartphones preconfigured to keep work data separate from personal data. COBO devices do not allow personal data on the device but this can be an attractive model for organizations operating in regulated industries (such as healthcare). Many businesses mix and match strategies according to regulatory restrictions, employee responsibility or geographical location, type of data, and other factors. BlackBerry enables them to do that, offering BlackBerry 10 devices as well as cross-platform management software such as BES12 and Secure Work Space by BlackBerry® for iOS and Android™ for managing BlackBerry, iOS, Android, and Windows Phone® devices.

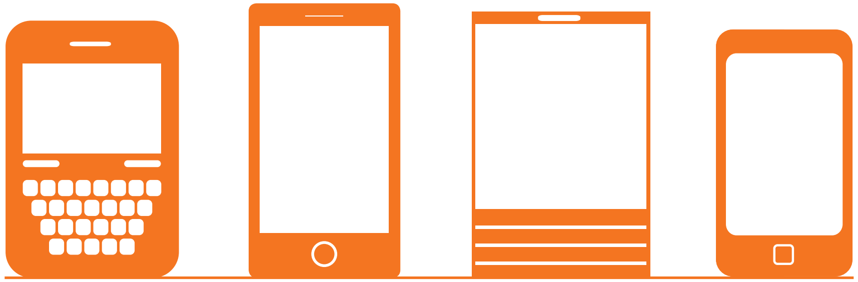
London-based market research firm Ovum predicted in 2014 that “informal (unmanaged and largely unrecognized) BYOD usage will slowly be displaced by a more managed approach, due to the introduction of more formal support models for employee-liable connections and devices in larger companies, as device management solutions for smartphones mature.”

Which device deployment approach will give your healthcare organization the best balance of security, productivity, and user satisfaction? Only you can make that decision, but one thing is for certain: BYOD is no longer the only option.

BYOD: The People’s Choice

BYOD is still a huge force to be reckoned with, mainly because few, if any, workplace programs can match the variety of consumer smartphones and the rapidity at which they become upgraded. However, while it certainly keeps employees happy, BYOD has not panned out as positively for the bottom line as originally hoped. For instance, employees are not as eager to pay all the costs associated with their personal device as once thought. According to a *2013 Forrester Research study*, which surveyed more than 3,000 information workers in Europe and North America, 35 percent of employees want to choose their own smartphone for work but do not want to contribute anything to the cost. Only 8 percent of survey respondents said they would pay the entire cost.

Companies have found that supporting BYOD in fact is quite expensive. A 2013 survey conducted by *Gartner Inc.* revealed that 81 percent of organizations reported that mobility had increased the helpdesk workload. A wide-open corporate BYOD policy generates the need to support potentially dozens of different devices and operating systems, introducing management complexity that far exceeds device and application management costs associated with a more-controlled number of end user devices.



The complexity of managing many different devices and operating systems might explain why many companies have tended to dismiss the need for BYOD management. Seventy percent of companies in the United Kingdom, for instance, do not implement a formal BYOD program, according to a recent survey conducted by *Ovum*.

BES12, BlackBerry's cross-platform EMM software, can secure company data across multiple types of mobile devices and operating systems, and enables healthcare organizations to stop playing security roulette when they allow BYOD. However, BYOD is best suited to companies or particular employees involved in low-risk business endeavors.

COPE: A Good Balance

A formal BYOD effort starts with a consumer device and extends it to the work realm. COPE does the opposite. It begins with a company-supplied device, with IT carving out space for personal data. Happily for users, healthcare organizations can offer a wide variety of smartphones to their workforces, an option also known as Choose Your Own Device (CYOD).

COPE not only satisfies employees that want to use one phone for work and personal life, it's the best choice for companies who view mobility as a long-term strategic investment, say analysts. The flexibility of COPE allows organizations to control data access and use as their situation requires or the company grows. Organizations subject to rigid auditing or compliance requirements, for example, can reduce the number of devices offered or impose stricter rules for network access or data sharing. According to Gartner, companies that own employees' phones face less litigation because it's easier for them to impose specific data policies.

However, if the business environment allows it, COPE organizations can relax requirements. These companies might implement a mobile use policy closer to a BYOD environment, which is characterized by a diversity of devices and platforms and loosely enforced security.

A 2014 Gartner report entitled *Protecting Enterprise Information on Mobile Devices, Using Managed Information Containers* documented the ability of BlackBerry to support *COPE*. The report stated that "BlackBerry comes closest to offering a product to support COPE" because BlackBerry devices come with the BES12 operating system with built-in personal and work spaces with BlackBerry Balance technology . "Other container products do not support such a model," it stated.

With BlackBerry Balance, organizations can implement a successful COPE program. You will also want to compile a list of devices long enough to please employees – but short enough not to overwhelm IT. In addition, it's wise to issue a mobile device policy that outlines your expectations and guides employee device use. This mobile device policy can help prevent confusion and resentment over after-hours work, for instance – a problem at the crux of a suit brought by police officers against the city of Chicago for back pay.

COBO: Avoiding risks

A COBO strategy does not allow users to keep any personal data on their work-issued smartphone. No personal email, no Internet access, and no personal texting. COBO is best for companies who have a strong risk aversion or who must comply with stringent regulations. Health, financial, government, and other strictly regulated organizations might find COBO to be the best – or only – fit. Healthcare organizations and companies with European headquarters or branches might consider COBO to avoid running afoul of tighter privacy laws there and elsewhere.

The UK government's *Communications-Electronics Security Group (CESG)*, which publishes guidelines for securing mobile devices for regulated industries, in the *Bring Your Own Device (BYOD) Guidance: Device Security Considerations report*, outlines 12 areas that companies should consider when they plan how to protect themselves from legal liability.

> “COPE not only satisfies employees that want to use one phone for work and personal life, it's the best choice for companies who view mobility as a long-term strategic investment, say analysts.”

It's Your Choice

Your healthcare organization may be choosing among BYOD, COPE, and COBO as an organization-wide standard for the first time. Or it may be moving from one deployment model to another. Or, as is very possible, you may choose to deploy more than one of these models to accommodate different employees: COBO for nurses who leave their smartphones at the hospital for the next shift, COPE for physicians and administration, BYOD for transporters and housekeepers.

BES12 can accommodate all these device deployment models, giving you a single management console to oversee a mix of corporate and BYOD BlackBerry, iOS, Android and Windows Phone devices. BES12 provides a seamless separation of work and personal content that perfectly balances end user and enterprise needs without compromise.

Billy Ho is Executive Vice President, Enterprise Products and Value Added Solutions at BlackBerry where he leads the Enterprise Product Management and Software organizations.

A Primer for Deploying EMM in Your Healthcare Organization

By David Moellenkamp, Senior Director, Solutions Development, BlackBerry

An Enterprise Mobility Management (EMM) solution is the software that IT uses to oversee a company's mobile devices. If you're thinking of changing your mobile strategy, you'll have a lot of complex decisions to make about your next EMM solution.

According to the market research firm *Ovum*, one of the biggest mistakes organizations make in choosing new mobile technology is molding their business to a product instead of the other way around. You should first decide on a mobile strategy, then find the technical solution to match it. Because most organizations use a mix of mobile devices and strategies to satisfy different roles, goals, and even geographical locations, the best EMM solution is one that can support all possible scenarios, says Ovum.

EMM: A Quick Overview

EMM is an umbrella term for a host of mobile software technologies. The main ones are mobile device management (MDM),mobile application management (MAM), and mobile content management (MCM).

MDM is control of the device itself; think password setup, device lockout and wipe, built-in data encryption, and over-the-air (OTA) provisioning. Regardless of how mobile devices are deployed to your employees – whether BYOD, choose your own device (CYOD), corporate owned, personally enabled (COPE), company owned, business only (COBO), or a mix of these deployment models – security experts consider MDM a minimum requirement for successfully managing a mobile workforce.

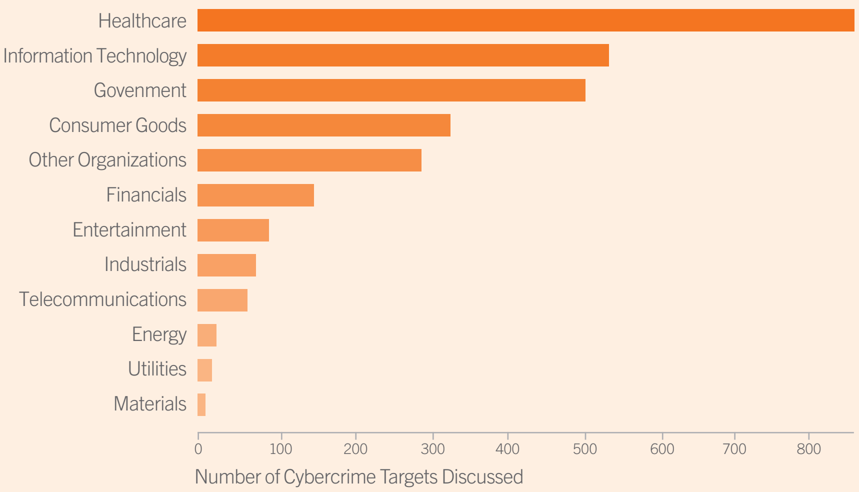
> Many companies find themselves buying a patchwork of different MDM, MAM and MCM tools. However, a single EMM console can save a lot of administrative time and hassle.

MAM software gives the mobile administrator centralized control over the deployment and management of the apps on your fleet of mobile devices. It assists with software licensing, configuration, and usage tracking. MAM software enables the IT administrator to limit what types of applications are able to be downloaded, based on IT policies.

MCM software focuses on secure document management and access to content on the devices. In addition to productivity apps, your organization might also want to provide such MCM features as an enterprise application store or a private, company cloud for secure file storage and exchange.

Many companies find themselves buying a patchwork of different MDM, MAM and MCM tools to address various mobile device deployment needs. However, the ideal EMM platform controls all the mobile tools deployed in your organization from one console. BES12 is the EMM platform that delivers this platform control from one console, saving you a lot of administrative time and hassle.

Cybercrime Targets by Industry (January 1 – May 15, 2014)



Source: SANS Analyst Program, SANS Institute, December 2014

First Steps

For a smooth EMM deployment, experts recommend a few first planning steps:

- **Define your business objectives.** What does your organization hope to gain from a new mobile solution? Do you need to speed up certain processes, improve sales or customer service, improve compliance with industry regulations, or rein in risky mobile practices that might expose company assets? Create a plan to gain agreement among stakeholders on the "vision." Scope out resources, establish a budget, and integrate the EMM project with strategic IT and business plans.
- **Make a list of desired technology.** Ask your IT group to develop a plan for implementing the objectives through EMM software and services. BlackBerry recommends that solutions include physical access security, authentication, end-to-end encryption, remotely manageable hardware controls, personal space and work space separation, and secure applications. BlackBerry also believes that enterprises should explore how to use EMM features to mitigate legal risks that healthcare companies can face from the insecure use of mobile devices in the workplace.
- **Consider extra needs.** Will you need custom development to achieve your objectives or help migrate an existing mobile infrastructure?

> Futureproof your EMM deployment with features such as secure voice, secure mobile messaging, mobile collaboration and split billing.

- **Future proof.** If your budget allows, incorporate the best available technology into your wish list to ensure maximum productivity and security now and in the future. Some of these features might include secure voice, secure mobile messaging, mobile collaboration, and split billing.
- **Don't forget the users.** If users don't like the technology, they can break the "best" EMM implementation by finding ways around the new rules. Along with increasing productivity and securing corporate assets, your goal should be to make your employees happy.
- **Test, test, test.** Before you can deploy your EMM solution, create and implement development and test environments and run tests of the solution in your environment.

Seek User Feedback

After you have run tests on your EMM solution, it's time to seek user feedback and, finally, deploy your EMM solution on a wider scale. Provide a self-service portal and let users set up their own devices to help them feel more a part of company policies. You will want to set up a mechanism for users to send you their feedback – whether it be via email, a web form, or a feedback survey.

The final step is revising the deployment in response to feedback, risks, and changing business requirements. You'll want to measure performance, monitor use and compliance, and refine governance processes.

Device Care and Feeding: The Usage Policy

Technology can protect mobile devices – think remotely wiping devices – but it can go only so far. The rest depends on user behavior. That's why as part of your EMM deployment it's important to provide users with a clear policy on corporate expectations when they use a mobile device to conduct company business. Along with standard requirements such as immediately reporting a lost or stolen device, provide as much detail as possible for various scenarios. For instance, if your devices are corporate owned but personally enabled (the COPE strategy), your policy should state what users can download into the personal space on their smartphones and how users can expect the company to treat their personal information.

Policies should also set out what users can expect from the IT department, especially for a BYOD device. For instance, IT might be willing to configure most aspects of the smartphone such as Wi-Fi® access, email and calendar, but the user might be directed back to their carrier for certain other support issues.

For more EMM advice, download the *BlackBerry EMM Realities kit* ➔ at *http://el.blackberry.com/emmrealities_index* that includes a collection of resources, templates, sample policies, and guides covering just about every aspect of deploying mobile hardware and software in the enterprise.

David Moellenkamp is Senior Director, Solutions Development at BlackBerry and is responsible for providing industry leading solutions to the mobility challenges that face enterprise customers, enabling them to unleash their mobile productivity.

Containerization: Finally, A Way To Keep Work Separate

By Jay Barbour, Security Director, BlackBerry

More healthcare workers than ever use a personal mobile device to get work done and improve patient care. While most healthcare organizations love the extra productivity this blurring of work and personal lives brings, what many organizations don't realize is how risky the practice can be to patient data.

Mixing healthcare applications that use patient records with personal apps on smartphones and tablets invites protected health information (PHI) leakage – employees unwittingly exposing sensitive patient data through all sorts of mostly well-intended activities performed on their mobile devices at work. For instance, a healthcare employee uses a non-secure instant messaging app to cut and paste a patient diagnosis to send to a clinician currently with that patient. Or when an off-duty doctor receives an email on his smartphone containing an attached sensitive patient record. Since this is after hours, he forwards the record to his home PC to read and respond on a large screen, exposing the data to malware and a range of other security issues on that untrusted PC.

Unfortunately, some of these data leaks stem from malicious intent. A healthcare worker copies prescription information into a personal webmail to commit prescription fraud. Or a hospital worker forwards the health records of a recently-admitted celebrity to the paparazzi – a blatant violation of HIPAA.

Finally, using a personal device risks that critical work applications such as paging apps get accidently deleted or misconfigured by children playing with the device, for instance. This can happen unbeknownst to the doctor on call, who still thinks he is reachable in an emergency.

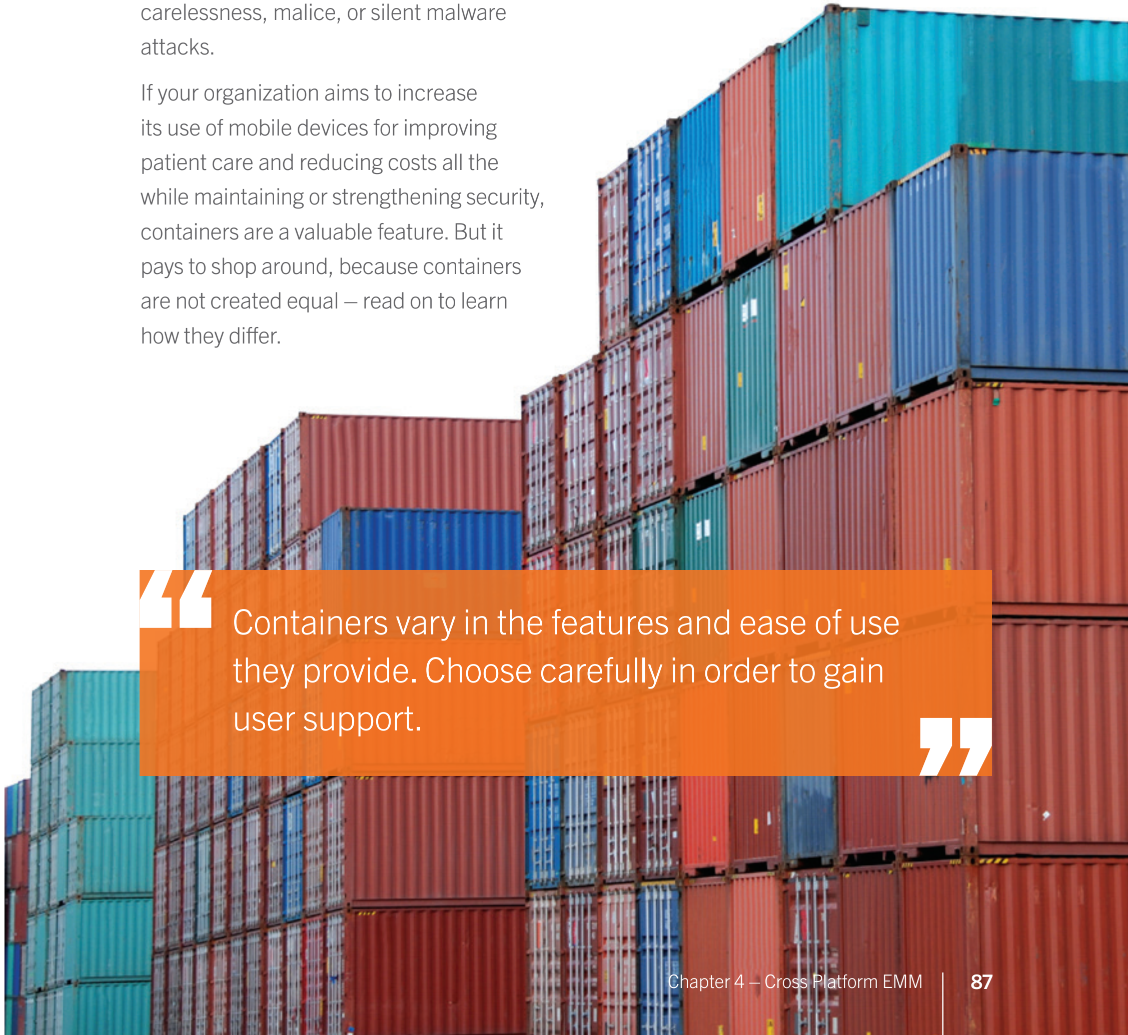
Leaks Here And There

To protect against these common data loss issues, an increasing number of Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) providers are offering a security capability called containerization. Container technology keeps healthcare applications and data separate from personal ones through data encryption and application barriers built into the operating system. This way, users can't accidentally lose PHI through carelessness, malice, or silent malware attacks.

If your organization aims to increase its use of mobile devices for improving patient care and reducing costs all the while maintaining or strengthening security, containers are a valuable feature. But it pays to shop around, because containers are not created equal – read on to learn how they differ.

The Container Store

Containerization began as a method of tagging individual pieces of information as private in order to protect it. Today's best implementations are a lot more sophisticated, with partitions built into the mobile operating system itself, making the security technology almost invisible to users, even while clearly partitioning work content from personal so there is no confusion.



> Containers vary in the features and ease of use they provide. Choose carefully in order to gain user support.

> Smartphones haven't been targeted by hackers as much as PCs. But as more business is conducted over mobile devices, this will change.

Containerization at the OS level also enables end-to-end management of the device using technology that is specific to the device OS. In other words, administrators enjoy easier and simplified management, in part because it is no longer necessary to manage the entire device. Only the work space container needs to be managed, and it is secure by default, so not a lot of configuration is needed.

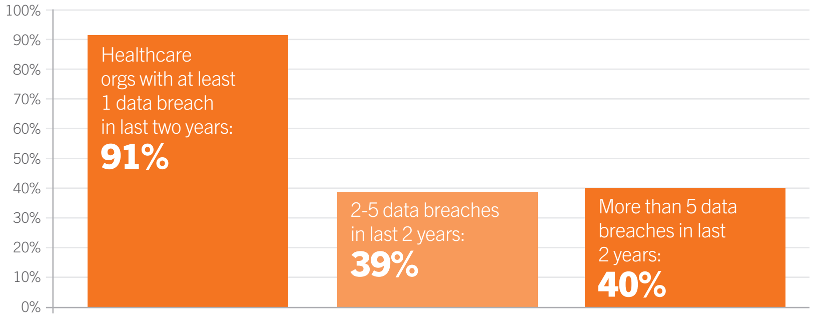
Containers give employees the freedom to use their smartphones as they normally would while providing the work space security that IT requires. Users can download and run any application they like without worrying about work data. The data in the work container is fully encrypted, managed, and secured.

Documents containing patient data, EHR/EMR applications, and content are locked. Nothing from the work space can be copied and pasted, forwarded, or offloaded onto a thumb drive. Healthcare mobile device IT policies secure and control the work space.

Any data that is generated in the work space is automatically saved there as well. Users who try to move PHI, or any other work data for that matter – for example, by cutting and pasting a work email into a personal document – are blocked with a message reminding them that the activity is forbidden. Similarly, personal data is isolated in the personal space – unless an administrator has set up the work space to allow data from the personal container to cross over.

Data Breaches in Healthcare Now Mainstream

Data breaches cost healthcare industry $6 billion/year; avg impact of data breach per organization is $2.1 million.



Source: Ponemon Institute, May 2015

A well-designed container implementation gives users a familiar smartphone interface and doesn't interfere with productivity. The work and personal spaces look like typical home screens, each populated by their own apps. Users can quickly move back and forth between the screens with a single gesture. The best container implementations also bundle a full suite of productivity tools and apps out-of-the-box, so employees are immediately productive without any complicated setup or additional IT costs.

What Can IT See?

Containers address another concern with Bring Your Own Device (BYOD), Choose Your Own Device (CYOD), and Corporate Owned, Personally Enabled (COPE) smartphones: user privacy. Understandably, users want to keep their personal information private, even on devices that their organization supports or supplies. Employees worry that IT won't respect their privacy and might even change or wipe personal data.

A good containerization implementation keeps IT out of the users' personal content. IT can isolate work applications, disable certain functions of apps within the work container, and wipe information within the work space without affecting personal user data.

How BlackBerry Does Containerization

All the latest BlackBerry smartphones have containers built into the BlackBerry 10 operating system. BlackBerry® Balance™ technology splits work and personal applications into two separate containers that users can toggle with one tap. Work data is encrypted and stays in the work container; users can engage in any personal activity that they like in the personal container, including emailing, texting, and social networking. So you don't have to switch back and forth between containers for common tasks, the BlackBerry® Hub interface shows all your emails, contacts, tasks, and notes – both work and personal – in a single unified view. But it restricts the ability to cut and paste sensitive work data – such as patient information – into applications in the personal container.

The Secure Work Space by BlackBerry® for iOS and Android™ is BlackBerry's version of BlackBerry Balance for non-BlackBerry smartphones. This means that every smartphone in use at your organization, whether company-supplied or BYOD, can keep work data safe and separate from personal activities. Using BES12, you can administer all the containerized smartphones – BlackBerry, iOS, Android and Windows Phone – from a single management console.

Containers help protect employees and organizations protect corporate data from exposure or theft, while keeping personal data personal. The work and personal spaces are contained in their own safe space, avoiding the possibility of a dangerous crossover.

Jay Barbour is a Security Director at BlackBerry, bringing more than 15 years of security experience in his work with government agencies, strategic and carrier sales teams, and key customers to champion security policies.

Healthcare Provider Chooses BES12 Enterprise Mobility Management for Security and Productivity

Industry:
Healthcare

Region:
North America

Company Size:
Large

Solution:
BES®12, Secure Work Space for iOS and Android™, BlackBerry® Balance™ technology, BlackBerry® 10 smartphones

Mackenzie Health

Based in Southern Ontario, Mackenzie Health is a regional healthcare provider that serves a population of over half a million people receiving approximately 92,000 emergency room visits a year. It has been nationally recognized for its commitment to both safety and quality patient care, with numerous awards and accreditations to its name. Mackenzie Health operates the Mackenzie Richmond Hill Hospital and five community health sites and has nearly 3,000 staff and physicians. In 2019, it plans to complete construction of the new Mackenzie Vaughan Hospital, a state-of-the-art facility which will employ over 1,800 staff and 100 physicians.

The Challenge:

Mobile devices have become ubiquitous in enterprise, but for businesses in regulated industries they represent a unique set of security concerns. Data and communications are subject to a number of stringent guidelines, all of which must be met while maintaining usability. This is easier said than done, particularly in organizations which blend bring your own device (BYOD) and corporate owned, personally enabled (COPE) deployment models, as Mackenzie Health does.

With six – soon to be seven – active locations, the IT professionals at Mackenzie Health have a massive fleet of mobile devices to manage. Security is paramount when connecting these devices to its networks, as Mackenzie Health's employees frequently deal with highly sensitive healthcare information. Just as important as security, however, is usability – if measures are too stringent, they will have an adverse effect on the productivity of the clinicians and staff.

"A lot of our challenges and needs are universal across hospitals; my counterparts around the world have the same challenges from a clinician and administrator perspective," said Mackenzie Health Executive Vice President and Chief Administrative Officer", Richard Tam. "We need to be assured that our mobile solution complies with strict patient privacy and confidentiality regulations without sacrificing productivity."

Key Benefits

- Offers support for both BYOD and COPE deployment models
- Ease of deployment for IT
- Provides secure connection to hospital systems, resulting in greater productivity for staff
- Enables compliance with all relevant healthcare industry regulations, including HIPAA

The Solution:

Already long-time customers of BlackBerry, decision makers at Mackenzie Health turned to BES12 to manage its expansive network of mobile devices. This multi-OS EMM solution is capable of managing any mobile deployment model, from BYOD to COPE, and offers seamless, secure support for any devices that the staff at Mackenzie Health needs to connect to their network, including Android, iOS, Windows Phone®, BlackBerry OS and BlackBerry 10 smartphones.

"We upgraded to BES12 so we can support any device platform our doctors choose. We issue BlackBerry 10 smartphones to our physician leaders, administrators, and managers, but the rest of our physicians and staff can bring their own devices," said Tam. "Any device that comes into our network has to connect through BES12, which provides end-to-end security for our BlackBerry 10 smartphones and a secure layer using Secure Work Space for iOS and Android devices."

"Together with BES12, BlackBerry 10 smartphones offer us the most secure end-to-end mobile infrastructure for our staff," said Tam. "We reviewed several MDM platforms, but ultimately chose BES12 for the security and peace-of-mind it offers us."

Mackenzie Health's Benefits:

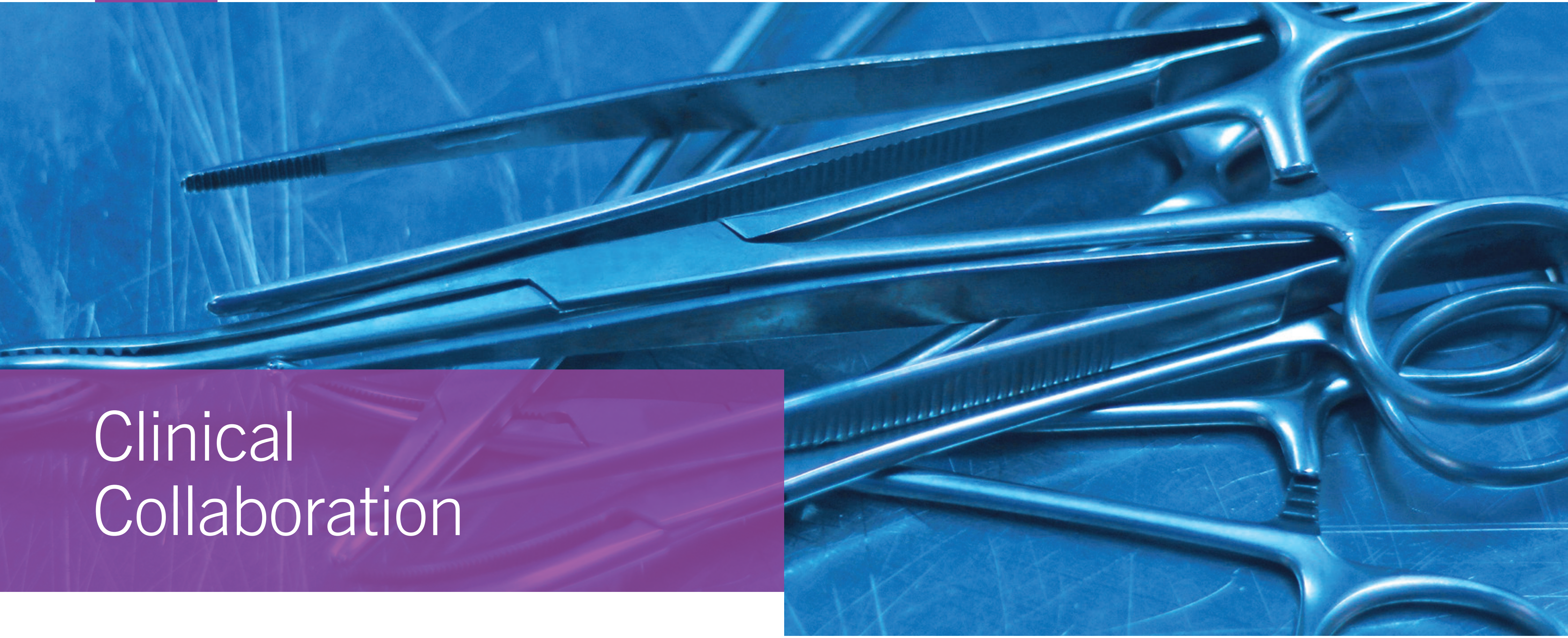
Thanks to BES12, physicians and staff at Mackenzie Health's many facilities are allowed a range of choice in their devices. Physician leaders and staff who are provided with a BlackBerry smartphone can choose from the BlackBerry® Classic, BlackBerry® Passport, or BlackBerry® Z30 offering choice between an all-touch and physical QWERTY keyboard. Employees who would prefer to use their own devices, meanwhile, can tap into the organization's BYOD program in order to do so.

Thanks to BlackBerry Balance on BlackBerry 10 smartphones and containerization through Secure Work Space for iOS and Android, personal information and corporate information such as patient data are kept separate, avoiding many of the privacy concerns associated with BYOD. Mackenzie Health's IT administrators, meanwhile, can visualize and manage their entire mobile deployment from a single, intuitive console equipped with an attribute-driven, endpoint-permissions model. This gives them thorough control of all applications, data and devices on their network.

"BlackBerry offers us uniquely secure end-to-end mobile infrastructure for our staff, but for all those who aren't issued a BlackBerry smartphone, our BYOD program allows us to securely and effectively manage connectivity to other devices like iPhones, iPads, Android phones and tablets through BES12," said Tam.

> BlackBerry offers us uniquely secure end-to-end mobile infrastructure for our staff, but for all those who aren't issued a BlackBerry smartphone, our BYOD program allows us to securely and effectively manage connectivity to other devices like iPhones, iPads, Android phones and tablets through BES12.
>
> **Richard Tam, Executive Vice President and Chief Administrative Officer, Mackenzie Health**

Chapter 5



Clinical Collaboration

Mobilizing Clinicians for Better Patient Care

By Dr. Karim Jessa, Chief Medical Information Officer, Hospital for Sick Children

Communication breakdowns in hospitals can have serious consequences. An estimated 400,000 deaths occur in the U.S. each year because of medical mistakes – a number that ranks as the third-leading cause of death in the country. Miscommunication is one of the main drivers. A recent report attributes 70 percent of treatment delays and sentinel (disease-indicating) events to a communication breakdown.

Hospitals and clinics are making efforts to improve communication and collaboration, but progress is not occurring fast enough – in part due to a lack of secure, reliable and viable options.

Clinical Collaboration in a Mobile World

Collaboration, as defined here, is the ability for doctors, nurses, and other clinicians to securely access patient information on mobile devices and work together with other healthcare practitioners to deliver better patient care.

When healthcare organizations mobilize information sharing and communication, benefits include: reduced emergency room wait times, improved communication and productivity, enhanced security for patient records, and increased focus on patient care. Current mobile technologies give healthcare providers the tools they need to do their jobs efficiently, allowing them to spend more time with patients by consolidating communication and information access to one platform.

> “The dreaded “Batman Belt” that clinicians wear to hold pagers, Wi-Fi phones, badges and a myriad of other tools is more complicated (and heavier!) than it needs to be.”

A variety of healthcare organizations can benefit from mobile collaboration between their clinicians, including first responders, home care providers, therapists, doctors and nurses.

Challenges to Mobile Collaboration

The healthcare industry is plagued with inefficient processes. For example, the process of paging a doctor (which seemed like the apex of sophistication well into the 1990s) is painfully slow and cumbersome compared to new options. Forcing clinicians to use a central switchboard is not conducive to good workflow.

However, because healthcare environments are large and fragmented, change can be difficult and slow. Patient history and information is stored in many different forms in many different places. Legacy infrastructure (like pagers and Wi-Fi® phones) is expensive to replace.

In addition, some well-intentioned technology solutions have hurt productivity instead of helping it. “Alert fatigue” is a great example: unimportant and incorrectly routed alarms have become the proverbial “boy who cried wolf” of today’s hospital, potentially distracting healthcare providers. On the information technology (IT) side, burdensome security protocols and inconsistent Wi-Fi/wireless coverage and mobile devices prevent better solutions in the workplace. Clinicians would rather consolidate to one device rather than wear a “toolbelt” to hold pagers, Wi-Fi phones, badges, and a myriad of other devices.

Clinicians Bring Their Own

In response, frustrated professionals are bringing their own consumer devices and apps to work. Many doctors in the United States are using smartphones to communicate with patients and colleagues (98 percent, according to the *Spyglass Consulting Group* report *Point of Care Computing for Physicians 2014)*. A majority of nurses are using personal smartphones for clinical communication (69 percent, according to the *Spyglass Consulting Group* report *Point of Care Computing for Nursing 2014)*.

> Unimportant and incorrectly routed alarms have become the proverbial "boy who cried wolf" of today's hospital, distracting providers throughout their shifts.

By bringing their own devices, healthcare providers have initiated a better solution in their quest to improve patient care. However, they now need their IT departments to support these devices, secure them, and show the healthcare staff how much more they can do.

A New Approach

Exciting new mobile apps and devices are coming to market all the time, offering elegant solutions to healthcare's entrenched problems.

Information Sharing

According to a recent health survey ›, 79 percent of physicians rated information access as the most important thing they need to improve patient care. In a clinical setting, information sharing includes secure file sharing for X-rays, scans, prescriptions, patient medical history, doctors' notes and instructions, and so on. Information sharing also includes point-of-care reference tools (such as PEPID, Lexicomp, or Epocrates), and workflow solutions that help clinical teams collaborate on care plans.

A number of apps address this need to share information, including various imaging viewers. With these apps, clinicians can view and interact with medical images and other content, and collaborate on diagnoses and treatments.

Communication

One of the reasons why consumers love mobile devices is the choice of communication channels that they offer: voice and video calling and conferencing, email, and messaging. In a clinical setting, they do all that, plus they can also provide smart and personalized alerts, alarms, and notifications.

ThoughtWire's Ambiant™ Machine Intelligence platform is helping nurses and doctors in Mackenzie Health's Innovation Unit mobilize workflows and fundamentally change the way clinicians communicate with each other and care for patients.

The BlackBerry solution has helped a leading US medical center significantly reduce its STEMI heart-attack response times. At the same center, an in-house built application for BlackBerry called MyRooms ensures nurses are assigned to their patients via mobile device and receive only relevant alerts.

Security

Forrester identified that the top three risks to securing healthcare information are related to employees using their personal devices at work: the devices themselves, consumer apps, and self-provisioning by employees.

Yet, with the right Enterprise Mobility Management (EMM) solution, mobilizing information and communication can actually improve security. For example, BES12 enables a highly capable and secure mobile environment with device, app, and content management; auditing and archiving; and firewall and encryption security.

BBM® Protected is a unique offering that that protects corporate data end-to-end with additional encryption for BBM messages sent between smartphones, whether they be BlackBerry, iOS®, Android™, or Windows Phone® smartphones.

Physical Logistics

Providing mobile devices to clinicians also makes common sense for collaboration. When healthcare providers discover that they can do more with one device, they can be more productive wherever they are. And when every clinician has a device, real-time communication helps workflows run smoother and faster.

Mobile Means Opportunity

Mobile device use provides a huge opportunity for healthcare providers for better diagnosis, better care, and better outcomes. The potential impact on productivity and efficiency is too big to ignore. Now is the time to investigate and implement new solutions.

Dr. Karim Jessa is an Emergency Physician and Chief Medical Information Officer at the Hospital for Sick Children. He is also on staff at North York General Hospital. He has a special interest in Clinical Information Systems and how the use of this technology can improve how Healthcare is processed and delivered.

Mobilizing Nurses: The Heart of Your Hospital

By Sara Jost, RN, Senior Enterprise Solutions Manager, BlackBerry

A recent report by *Spyglass Consulting Group* found that 69 percent of nurses are using their personal smartphones at work, yet 95 percent of those surveyed said that their information technology (IT) departments weren't willing to support them.

Why are nurses using smartphones? Simple: mobile devices help them do their jobs more efficiently. That's critical in an environment with escalating costs, resulting layoffs and labor shortages, increasing demands for documentation, inefficient workflows, and legacy systems that haven't kept pace with technology improvements.

Administrators and IT departments aren't just unsupportive; they're pretending like it isn't happening at all. That's not only unreasonable, it's also:

- **Unfair** to expect nurses to use their own phones for work when there's an accompanying legal burden, and no formal guidelines in place to reimburse them for on-the-job costs, damage, or loss.
- **Inefficient** for nurses, doctors, and other medical staff in the clinic or hospital to have to each build their own network by exchanging phone numbers.
- **Irresponsible** to lose accountability by not tracking and archiving staff communication or the history of care delivered because there's no backend support system.
- **Dangerous** due to security concerns. If IT doesn't secure personal smartphones that healthcare staff bring to work, then private medical information is vulnerable, putting the hospital at risk of serious liability and reputational concerns.

> “Hospitals that focus their tech investments on nurses can hardly go wrong. With 4 nurses for every 1 physician in the typical hospital, mobilizing nurses has much bigger ROI potential.”

If the main goal of a hospital is to provide better patient care, and smartphones help nurses do that, then it's time for IT and administration to get on board.

Smartphones on the Sly

Nurses care about patients. After a 12-year career as a registered nurse, I know that nurses are going to do whatever they can to provide the best possible care. They are the “MacGyvers” of the healthcare world, improvising with whatever they can find to do what needs to be done.

That's why the majority of nurses are using their personal smartphones. They're calling and texting each other, doctors, therapists, and the entire care team where they work. They're accessing electronic medical reference materials. They're creating calendar events to remind themselves to give medications to patients or when their patients have tests. They're creating workarounds to get past inefficient workflows to do more, faster.

IT departments and clinical administrators resist the idea of supporting personal devices for many good reasons. IT is concerned about the auditability and security of personal devices – and rightly so. But this concern is not a reason to ignore the trend. If anything, auditability and security concerns are why they need to implement an Enterprise Mobility Management (EMM) solution to secure all the devices on their network and clinical collaboration tools like messaging, voice, video, file, and image sharing.

Many administrators believe it's their responsibility to provide the technology for work, so they should be the ones choosing the work-supported devices. While that's definitely an option, the longer that decision process takes, the more personal smartphones will come in under the radar.

Nurses today spend substantial time on the phone to verify simple information. Automating the process can speed things up immensely. “I could ignore a voicemail for a thousand years, but when I get a text on my phone, I'm on it,” said one nurse.

(BlackBerry research, Sept. 2013)

Consult Nurses about Technical Investments

Meaningful Use regulations are spurring hospitals and clinics in the U.S. to update their healthcare technology. Our research has shown that 66 percent of hospitals are making investments to optimize workflow processes to enable patient-centered care. These investments are in workflow optimization (66 percent), interoperability (49 percent), medical device integration (26 percent), and bar coding medicine administration (22 percent).

As hospitals make these investments, nursing input is critical to success.

First, nurses represent the voice of the patient. They are the ones planning, documenting, communicating, and coordinating patient care; administering medications; educating patients about their medical conditions; and providing advice and emotional support to patients' family members. Nurses can give you the inside track on the patient's experience and patient safety.

Second, nurses are the main users of electronic medical records (EMRs). Nurses collect, document, and reference patient history, and vital sign data. In addition, most of the increased documentation requirements (due to Meaningful Use compliance, third-party reimbursement, and protection from litigation) are falling on nurses, forcing them to become "data collectors." Yet, 44 percent of nurses interviewed say it's difficult to integrate images within EMRs, 52 percent complained their EMR vendors have not invested in speech-enabling their clinical applications, and only 62 percent believe that the application development tools provided by the EMR vendors are sufficient to support nursing workflow processes and tasks at point of care.

Third, nurses have a deep understanding of clinical workflows and tasks. For example, our research found that while smartphones do support nursing workflows, tablet computers don't – at least not yet. First-generation tablets are too big, too heavy, and too fragile. The battery life is too short, there's no good method for data entry, and there's a lack of clinical apps. Rather than spending a lot of money on something that won't get used, healthcare administrators should give nurses a trial run with a few solutions and see what works for them.

> Nurses represent the voice of the patient. Their input is vital as hospitals invest in mobile technology.

Enable the Heart of your Hospital

An IT department that focuses its technical investments on nurses cannot go wrong. Providing nurses with mobile devices has a much bigger return-on-investment potential. There are more nurses: 13 million in North America, and four nurses for every one physician in a typical hospital environment. They are at the center of things: escalating healthcare costs are impacting nursing staff the hardest, because that's often where hospitals and clinics cut costs.

> Hospital alerts today are so frequent and unfiltered that a nurse can get up to 100 notifications per 8-hour shift, creating alert fatigue. "At the end of the day, I want to drop the phone in the toilet and walk away," said one nurse.
>
> (BlackBerry research, Sept. 2013)

Increasing documentation requirements also fall on nurses' shoulders. Our research showed that currently, nurses complete less than 50 percent of documentation at the bedside. Mobile technologies will help more of it happen in real-time, meaning it can be more comprehensive and accurate than if the documentation is done after the fact at the desktop computer at the central nursing station. It also means nurses would be able to spend more time with their patients and less time sitting behind a desk.

Nurses are already delivering better care through the use of their own smartphones. Instead of pretending they aren't, IT departments and healthcare administrators need to work with them to re-evaluate workflows, consider new solutions, and make stronger investments in the future of healthcare.

Sara Jost is the Healthcare Solutions Manager for BlackBerry. She has a background in eHealth/mHealth, research and is a Registered Nurse.

Lines of Contact: Selecting a Secure Messaging Option for Your Healthcare Organization

By Ryan Steeves, Senior Product Manager, BlackBerry

Communication is fundamental to healthcare, but as mobile technology continues to proliferate through multiple markets and industries, the inefficiencies within traditional healthcare communication models have become increasingly evident. In a 2015 *Spyglass Consulting Group report*, nearly 70 percent of clinicians who responded believed that their IT department was taking inadequate measures to address mobile computing and communication.

In the same survey, it was found that smartphone adoption among physicians is now nearly universal, at 96 percent. More importantly, these physicians use their phone as their primary means of contact, as opposed to traditional options such as pagers, fax machines, paging systems, and landlines. It isn't just professionals at the highest levels of healthcare who are solving their mobility challenges without their IT department.

As of 2014, the *Spyglass Consulting Group reports* that 67 percent of hospitals reported that their nurses also use personal smartphones at work to support clinical communications and enhance workflow. Because of a lack of a suitable internal solution, nurses turn to consumer messaging platforms or SMS in order to communicate about patients. While their actions are undoubtedly carried out in the best interest of the patient, they are not in the best interest of the organization. Although this unregulated mobile hardware and software allows healthcare employees to operate with greater efficiency, it also opens up the organization to a bevy of privacy, compliance, and security concerns. Ironically, this unregulated mobile device use also creates a host of new inefficiencies, because staff must operate outside of their organization's workflow in order to use their personal devices. Employees must exchange phone numbers or contact details with one another in order to connect that will lead to a high likelihood of errors and unnecessary repetition of notifications.

Data leakage aside, if mobile devices should fall into the wrong hands, there is also nothing to protect the information on these devices. And according to a September 2014 report by *Forrester*, lost or stolen devices are among the likeliest avenues through which healthcare information will be compromised, particularly given that a third of healthcare employees work outside the office at least once per week and 52 percent of employees store patient data on their devices.

> Lost or stolen devices pose a huge risk for data loss, since one-third of healthcare employees work outside the office at least once per week and 52% store patient data on their devices.
>
> (Forrester, 2014)

> 70% of delayed treatment events and sentinel events are the result of communication breakdown.
>
> (The Joint Commission, 2012)

Clearly, the use of non-compliant messaging platforms is unacceptable. But the alternative – to expect that employees simply suffer through the archaic platforms that their healthcare organization already has in place – is equally unsuitable. According to a 2012 report by The Joint Commission, 70 percent of delayed treatment events and sentinel events are the result of a breakdown in communication. In large part, this breakdown is because, traditionally, healthcare communication leaves little room for follow-up. That forces many nurses to create informal cheat sheets to record essential information and communicate it to fellow employees.

Alongside physicians, nurses are also subjected to a constant barrage of notifications from PA systems, medical equipment, phones, and more. In many cases, these frequent interruptions have led to a phenomenon the Joint Commission in their Sentinel Event Alert report refers to as *alarm fatigue*.

“The number of alarm signals per patient per day can reach several hundred depending on the unit within the hospital, translating to thousands of alarm signals on every unit and tens of thousands of alarm signals throughout the hospital every day,” the organization writes in Issue 50 of its Sentinel Event Alert publication. “It is estimated that between 85 and 99 percent of alarm signals do not require clinical intervention...clinicians become desensitized or immune to the sounds, and are overwhelmed by information – in short, they suffer from ‘alarm fatigue.’”

Constant noise from alarm signals can also affect patients. The World Health Organization found that a continuously noisy environment can lead to delayed wound healing, aggressive behavior, psychiatric symptoms, and increased re-hospitalization rates. It can also lead to an *increased risk of hypertension and ischemic heart disease* ➲.

Another study by Moore and colleagues found that surgical patients identified noise as the biggest irritant during hospitalization, and, postoperatively, surgical patients in a noisy environment require more pain medication than those in a quiet setting. Noise also interrupts sleep in hospitalized patients, some of whom are particularly vulnerable to sleep disruption.

In order to address all of these issues – alarm fatigue, noisy environments, inefficient communication, and the use of non-compliant messaging – healthcare providers must select a suitable secure messaging platform that can be deployed to their clinicians and staff. This deployment in itself represents a new array of challenges, because any option healthcare provider’s use must meet the following standards:

- **Usability:** Optimally, an organization’s secure messaging platform must be both easy to use and familiar to the majority of healthcare staff, and serve the goals of the enterprise. Healthcare employees are increasingly pressed for time; they’ve neither the bandwidth nor the will to learn and adopt a new, wholly unfamiliar system. The solution needs to include a full range of messaging features including the ability to collaborate between several users at the same time, by creating groups for example. It is also imperative that the security measures provided by this solution do not restrict its usability.
- **Multiplatform support:** The majority of healthcare employees choose to bring their own devices to work. But there are many entrenched platforms, too, that must be accounted for. The result is a diverse selection of different platforms. A suitable secure messaging option must operate across a variety of devices.
- **Auditing and reporting tools:** HIPAA requires that all healthcare communications be properly regulated and audited. A secure messaging option should also include easy-to-use auditing and reporting tools.
- **Data encryption:** To prevent data leakage or interception of potentially sensitive information, messages sent from one employee to another must be fully encrypted at rest on the device and in transit.
- **Cloud security:** Healthcare providers relying on cloud-based secure messaging need a solution that prevents patient information from being stored in the vendor’s infrastructure. With the latest onslaught of security breaches of customer data on both vendor and customer premises, healthcare providers are rightly concerned about pushing patient data into a vendor’s cloud.

Mobile Security Among Weakest Parts of Healthcare Organizations, Say Leaders

Security Controls	Very Effective	Effective	Total sum of Effectiveness	Not Effective
Network/Perimeter defenses	25%	51%	76%	25%
Application security	10%	62%	72%	10%
Database security	16%	55%	71%	16%
Endpoint protection (centrally managed)	19%	51%	69%	19%
Administrative (policies and procedures)	10%	58%	68%	10%
Data protection/Encryption	20%	47%	67%	20%
Contractual relationships with business associates	14%	50%	64%	14%
Vulnerability management	7%	53%	61%	7%
Security risk management framework	11%	48%	59%	11%
Identity and access management (IAM) controls	12%	44%	56%	12%
Training and awareness	10%	43%	53%	10%
Mobile security and access controls	8%	41%	49%	8%
Data breach detection solutions	4%	43%	48%	4%
Big data initiatives and data governance	3%	43%	47%	3%
Malware analysis systems/Honeypots	10%	37%	46%	10%

Source: SANS Analyst Program, SANS Institute, December 2014

BBM® Protected readily meets all of these challenges. BBM, the enterprise-class messaging platform upon which BBM Protected is based, has over 90 million active users a month, with an average response time per message of 8 seconds. BBM Protected offers a seamless front-end user experience and integrates perfectly with the other solutions in the BlackBerry enterprise portfolio. And unlike cloud services that store patient and other data in a central, hackable database, BBM Protected – and BBM for that matter – only encrypts and passes through data to be stored on endpoint devices, not in a single repository.

Alongside its intuitive, easy-to-use auditing and reporting tools, this level of integration is what sets BBM Protected apart from other messaging platforms on the market. With BBM Protected, BES®12, BBM® Meetings, and WatchDox® by BlackBerry®, an organization can manage everything about its mobile infrastructure from a single interface and conduct business with a single, trusted vendor for true end-to-end mobile security.

An example of this messaging platform in action is sharing patient data on-the-fly through organized BBM Protected chats, which teams can join and leave as shifts change. That way, all the history for a particular patient is readily available to whomever is assigned to them, but none of the data is stored on the device. Staff can be further organized into groups based on their position, or ones organized around a particular patient and persist as long as he or she is in hospital. This way, contact with required personnel is only a few clicks away if a consultation is required. BBM Voice, BBM Video or BBM Meetings can be used if a voice call is necessary.

Adding WatchDox by BlackBerry, a secure enterprise file sync and share (EFSS) solution, offers further value. Employees can edit, upload, and share electronic records and patient documents without ever leaving a patient's bedside – and without putting any of that information at risk. In short, WatchDox by BlackBerry provides everything a healthcare firm needs to be, both efficient and compliant.

Communication is core to the healthcare experience. It's past the time that healthcare providers start taking steps to ensure that communication is no longer stymied by organizational inefficiencies. By implementing a suitable, intuitive, secure messaging platform, hospitals and other healthcare providers can ensure that their employees operate more efficiently and more productively – and achieve better patient outcomes as a result.

Ryan Steeves is Senior Product Manager responsible for enterprise BBM, BlackBerry's secure communications platform, with particular focus on delivering solutions to the Healthcare vertical.

CASE STUDY

This Hospital Chose BlackBerry for Security, Coordination, and Better Care

Industry:
Healthcare

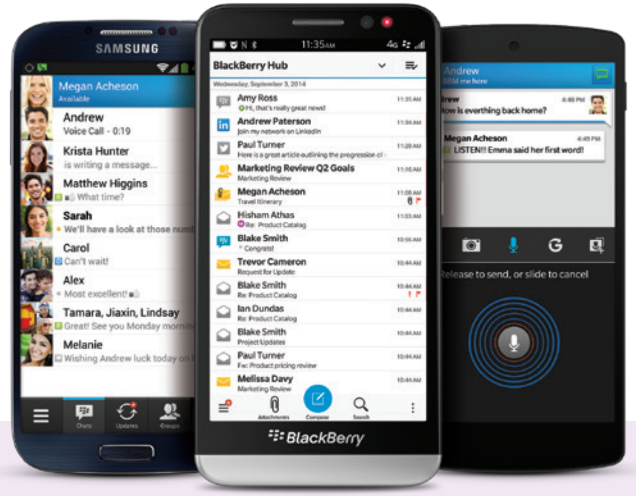
Region:
North America

Company Size:
Large

Solution:
BBM® Protected,
BES®12

Grand River Hospital (GRH) is one of Ontario's largest community hospitals and provides innovative, quality care to more than 700,000 residents of Waterloo Region and Guelph Wellington. GRH is a leading healthcare organization, offering cancer and renal (kidney) services; care for the most seriously ill and injured adults; services for mothers, newborns and children; emergency care; mental health and addictions; and care for older adults including rehabilitation. The Hospital is privileged to be a key partner in health sciences learning and has a rapidly growing role in academic and applied research. GRH patients benefit from the services of 3,400 staff members, 600 professional staff and 1,000 volunteers at the Kitchener-Waterloo and Freeport campuses as well as satellite locations in Waterloo Region and Wellington County.

GRAND RIVER HOSPITAL



The Challenge:

To attain the highest level of efficiency and the best patient outcomes possible, hospitals must enable employees to communicate with one another in real-time. Decision makers at Grand River Hospital understood this, but they also realized that the topic of such communication is most often patient care, which requires additional security to keep patient data private. In order to establish communication links between staff, they needed a solution that was compliant with regulations such as PHIPA (Personal Health Information Protection Act).

"Everyday text messaging would not work for us. We needed a service that's secure and encrypted so our patients' health information remains private," explained Kathleen Lavoie, Grand River Hospital's Corporate Director of Information Management and Chief Privacy Officer.

But they also needed a service that was easy to use. Since Grand River Hospital employs a mixed mobile deployment model, many doctors in the facility choose to bring their own devices to work. If Grand River's mobile communication solution didn't meet usability requirements, employees would simply see it as an obstacle.

"We don't control what devices physicians buy or use in the workplace. The hospital has a policy of BYOD" said Gary Higgs, Chief Information Officer at Grand River Hospital. "We needed a solution that is intuitive and easy-to-use for the clinicians all the while ensuring the security surround their communications."

Key Benefits

- Real-time secure communication helps to improve workflow and patient outcomes
- Easy deployment and management ensured minimal load on IT
- Full compliance with regulations such as PHIPA regardless of device
- BES12 and BBM Protected offer full support for mixed deployment model

The Solution:

Grand River Hospital needed a solution capable of meeting both their regulatory and usability requirements. After discussing the matter with physicians and testing the solution, the hospital decided to deploy BBM Protected. This powerful mobile messaging application is platform-neutral, and combines the familiar, full-featured BBM instant messaging interface with an added layer of encryption to ensure data security and compliance.

Grand River Hospital uses BlackBerry 10 smartphones for many of their management staff and some physicians, with the rest of their physicians operating on a BYOD model. In order to securely and efficiently manage these and all other devices in its operating environment, the hospital uses BES10 and is in the process of upgrading to BES12.

> “In addition to high-quality care, the security of personal health information is one of the most important responsibilities we must fulfil for our patients. We feel that BBM Protected will be a major benefit to care providers consulting each other about a patient’s needs, providing them timely information in a secure manner.”
>
> **Kathleen Lavoie, Corporate Director of Information Management/ Chief Privacy Officer, Grand River Hospital**

“We talked to our physician groups for about a year regarding the idea of giving them a tool based around secure communications,” explained Higgs. “We considered multiple options, but BBM Protected was the ideal fit for our requirements, as it’s secure, easy to use, and platform agnostic, allowing us to deploy it across the range of mobile devices in our environment.”

Grand River Hospital’s Benefits:

With BBM Protected, Grand River Hospital’s staff can communicate in real-time about patient status, significantly enhancing their workflow—whether they are using one-to-one or group chats. With BES12, the hospital will also fine-tune its security, giving itself the capacity to quickly and easily manage both COBO and BYOD devices. Thanks to the relatively low adoption requirements, deployment and security enforcement are carried out with ease on both the end-user and administrative side.

“The BlackBerry solution including BBM Protected and BES12 allows us to maintain the security and privacy of our patient data while empowering our clinicians with the tools they need to provide the best possible care,” said Lavoie.

“In addition to high-quality care, the security of personal health information is one of the most important responsibilities we must fulfil for our patients,” Lavoie added. “We feel that BBM Protected will be a major benefit to care providers consulting each other about a patient’s needs, providing them timely information in a secure manner.”

Getting Smart About Alerts and Notifications

By Mike Monteith, CEO, ThoughtWire

More stress is the last thing a hospital staff needs. But the Internet of Things (IoT) and all the data it creates can become a major source of stress if not managed properly.

Part of the IoT is the network created by smart sensors in healthcare machines that can measure, record, and transmit data. For example, new heart rate monitors alert nurses when a patient's pulse falls below a certain threshold. Smart beds know when their occupants have left their bed, and if that patient is at risk for falls, it can send a notification message to let an attendant know.

These sensors provide a tremendous opportunity to improve patient care, safety, and productivity. At the same time, there's now an avalanche of information available about patients and hospital environments.

That's where smart machine technology comes in. If we can filter the "noise" created by the IoT, we can get the right information to the right people at the right time.

> Smart alerting combines relevant hospital or clinic data that already exists, such as who's working, where are they right now, and which nurses are responsible for which rooms, with real-time events.

Alert Fatigue

Many early healthcare solutions took a "because we can" approach, collecting all the data they could and sending it to everyone who could receive it. That combination of unimportant information and wide distribution has bombarded healthcare providers with irrelevant alerts. The information overload causes distraction at best and blatant disregard at worst.

To put that into perspective, one of our customers, a 32-bed hospital, registers about 1,200 bed exit alarms per month. That adds up to nearly 15,000 events a year. If each event requires a 3 minute response, that's 45,000 person minutes each year, or 750 hours – much of that time is wasted. Luckily, there's a better way: smart alerting.

Smart Alerting

Smart alerting combines relevant hospital or clinic data that already exists, such as who's working, where are they right now, and which nurses are responsible for which rooms, with real-time events.

Critical response teams are a great way to illustrate this idea, for example, a heart rate monitor registers that a patient just flatlined.

Without the IoT and smart alerting, here's how that might play out. The heart rate monitor alarm goes off. A nurse or doctor hears the alarm, runs into the room, and pushes the code blue button, which lights up a console in the hospital dispatch office. The dispatcher uses the loudspeaker to announce the code blue alert to the entire hospital. Every individual on every code blue response team stops what he or she is doing, listens to the announcement, and then makes the decision whether to go to the room. Each person on the team has different responsibilities, which dictates what they need to do (for example, one person may need to find a crash cart that has all the tools they might need to save the patient's life such as a defibrillator, drugs, suction devices, and so on).

> Smart machine technology can interconnect all of the available patient data with real-time events as they unfold.

When the team arrives, they huddle up to gather information to decide on the care plan, either by looking through paper documents or logging into a computer.

Given today's technologies, this scenario is inefficient, wasting precious time when a life is at stake. It's also ineffective, because the code blue dispatcher has no way of knowing if the entire team has received the message and is responding, how far away they are, or when they will arrive.

With smart alerting, the scenario plays out quite differently. The heart rate monitor alarm goes off, which triggers a code blue event in the hospital's closed-loop system. Intelligent software determines who the appropriate responders are in hundredths of a second by analyzing information about who is on the team and who is on shift, and alerts all the right people through their mobile devices. Team members have seconds to respond (for example, 10 or 15 seconds) before the system alerts the next available team member. The systems can send patient history to team members to read en route, and use radio frequency identification (RFID) technology and location services to identify the closest crash cart.

Clearly, this smart alerting version of events is significantly more efficient. It's also more effective: when team members respond, the system knows who is on the response team and can communicate with them directly. In addition, the entire process becomes auditable, because the system captures all the data and tracks the activity.

Beyond Critical Scenarios

Smart alerting has benefits for non-critical situations as well. When a patient calls for help, a smart alerting system can use scheduling and location data to identify the nurse responsible for that room and notify the nurse directly. If that nurse is on a lunch break in the cafeteria, the system can alert another nurse. Some systems even incorporate video calling, so nurses can check in with patients directly before making the trip to the room.

Without smart alerting, the patient's call may be unanswered or delayed if no one's at the nursing station when the console lights up. Faster responses result in better patient care – and reduce the risk of patients falling, for instance, if they decide to get up themselves when help doesn't arrive. Smart beds can tell when their occupant has left the bed, the position of the side rails, and the inclination of the headrest. If anything is amiss, the bed can alert the appropriate nurse assigned to the room to check on the patient and make sure that the patient is safe.

How to get Smart

There are many different ways hospitals can get smart about alerts and notifications. Closed-loop smart alerting systems combine data from several sources and make decisions or start workflows. Data is available from the following sources:

- **Internet protocol (IP)-enabled systems:** HVAC for temperature control, lighting, security (locking and unlocking doors, closed-circuit surveillance, real-time location, and RFID technologies), and fire alarms and sprinklers.
- **Rooms:** Nurse call systems, unified communications for voice and video, integrated bedside communications capability (information displays and soft panels for code calling), and smart devices in the room such as beds, infusion pumps, heart rate monitors, and other telemetry.
- **Hospital information systems:** Store patient identity and medical history, clinical data, administrative data, scheduling, staff incidents, and more.

An important consideration is infrastructure. Secure mobile device management, ubiquitous Wi-Fi® networks, and identity verification systems provide the secure environment that's the foundation for these data-sharing solutions.

Expanding Possibilities

As the IoT expands and mobile technologies improve, we're starting to demonstrate what's possible. Not all hospital buildings can incorporate all the new technology today, but small investments can leverage existing systems and yield great results.

Smart machine technology can interconnect all of the available patient data with real-time events as they unfold. Currently, we have a unique opportunity to transform clinically relevant digital moments into dramatically improved patient care, patient and staff safety, efficiency, and productivity.

Mike Monteith is CEO and co-founder of ThoughtWire Corp. Mike's broad experience encompasses business and enterprise strategy, IT strategy, enterprise architecture and large-scale program implementation.

Mobilizing Clinical Images Securely

By Claudio Gatti, CTO Visualization, Enterprise Software and Healthcare, Lexmark

If a referring physician didn't have to wait a week to get the results of an MRI, how would that change patient outcomes?

Mobile technology is giving the healthcare industry the opportunity to improve the way it works by simply making things more available to the people who need them. The process of distributing diagnostic images – X-rays, MRIs, CTs, ultrasounds and others – is a case in point. The particulars have been similar across hospitals for decades. The images themselves were films or paper prints. Radiology departments had to take the images, analyze and interpret them and then mail or fax the images and reports to the requesting physician. Doctors and patients had to wait days or weeks for the results.

But now, the Web, mobile devices and mobile apps are speeding up the process and making the images themselves more accessible and also more secure.

> "Some hospitals stop from mobilizing images because of fear around security breaches. But today's solutions actually improve on the security of paper and film records."

Why Mobilize?

The need for cross-department and cross-enterprise information sharing is greater than ever before. This is particularly true for medical images. A universal medical image viewer meets this need by allowing clinicians to view any medical image, imaging report and related patient data anytime and anywhere outside of a picture archiving and communication solution (PACS) environment. Digital image access is no longer confined to the department that created the data.

Several trends are driving the shift from physical images to mobilized images: the push for universal patient records (UPR) and electronic medical records (EMR), plus the fact that recent advances in consumer technology have changed what's possible as well as people's expectations of how things should work.

Better Care

Universal medical image viewers allow hospitals to capture, manage, view and share all medical imaging-related content. That leads to better patient care, security and cost efficiency.

Mobilizing images results in better patient care because physicians and patients can get their test results faster and begin treatment sooner.

Mobilized images are also more accessible. Without mobilization, images are generally only available through a central computer or specific workstations within each facility.

Universal medical image viewers make images available across platforms, devices and facilities. They also add convenience and efficiency, enabling care providers to refer to the images more often, and allowing patients to access and keep their own records.

Universal medical image viewers improve collaboration as well, allowing physicians to easily share them with colleagues.

Better Security

The improvement in security that image viewers provide may come as a surprise. A common misconception that keeps hospitals from mobilizing images is fear of security breaches. But today's solutions actually improve on the security of paper and film records. "Zero-footprint" solutions or those that use cloud storage along with encrypted SSL protocols allow image viewing on smartphones and tablets while transferring nothing to the device itself.

Additionally, many solutions are compatible with enterprise-grade, single sign-on authentication. IT departments can further protect sensitive information by defining different roles for individuals and groups in the system, granting appropriate levels of access for each.

Cost-Effectiveness

Mobilizing clinical images through Web-based solutions is flexible, scalable and cost-effective. Care providers can access them from any Web-enabled device, including large and small phones, tablets and laptops, which support Bring Your Own Device (BYOD) policies. Pricing for cloud solutions is pay-as-you-go, so hospitals can add or remove users as their needs change and only pay for what they're using.

Accessibility Increases Use

Mobilization frees up the images so people across the enterprise can view them outside of a PACS or through a vendor-neutral archive (VNA) or other enterprise-class archives. Surgeons, particularly orthopedic surgeons, tend to interact with the images a lot, making decisions about care plans and patient options based on the image. Additionally, as more patients today are researching their conditions on their own, physicians can easily share the images with patients, walking them through their diagnosis and care options.

Mobilization also provides an easy path to including imaging in EMR solutions and UPR solutions which give patients access to their own records so they can easily share among doctors.

> Mobilizing clinical images makes it easy to include them in electronic medical records, giving patients access to their own records for sharing with their doctors.

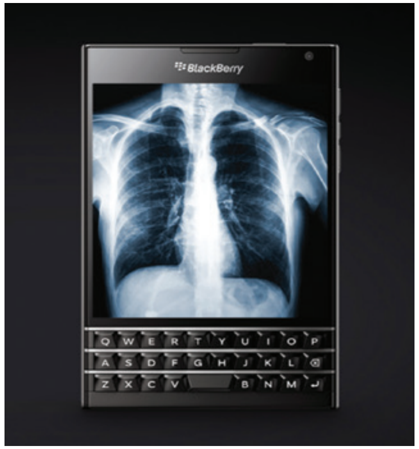
Mobilization also enables:

- Cross-enterprise image sharing for collaboration and second opinions
- Cross-enterprise image sharing for trauma transfers and other emergency cases, enabling decision- making on a case before the patient is transferred
- Referring physician image access, typically through a physician Web portal
- Image viewing across a health information exchange (HIE)

A Better Way

Mobilizing clinical images enhances patient care by speeding diagnoses and increasing accessibility and collaboration – between physicians and colleagues and between physicians and patients. Imaging solutions also improve security and keep costs down by enabling the ability to scale up or down as needs change.

When people work around a problem long enough, it can be easy to forget that it's a problem at all. That's true when we talk about technology and healthcare and particularly with diagnostic imaging. The lag time between imaging and the report and the inaccessibility of the images themselves are now clearly problems because mobilization offers a better way.



Claudio Gatti is the CTO of Visualization, Enterprise Software and Healthcare at Lexmark. He is the former co-CEO of Claron Technology which was acquired by Lexmark.

Leveraging the Potential of BYOD

By Andrew Silver, CTO, Tango Networks

The phenomenon of BYOD has not permeated health care environments the way it has other workplaces. There have been some very good reasons for that, but new technologies available today make this worth reconsidering.

Because of the need to respect patient privacy and the confidentiality of patient information, many healthcare organizations have been reluctant to take chances when it comes to communications devices and services. They must uphold HIPAA compliance in all aspects of their operations and often see risks in the use of employee-owned mobile devices outweighing benefits.

With that said, what are those benefits? A key one is user proficiency with the communications device they use in connection with their job. The phone an employee brings to work in a BYOD scenario is one that the employee already knows how to use, is comfortable with, and is experienced at using. Rather than have every employee be issued an expensive mobile device made by a certain manufacturer and tied to a specific network, BYOD enables an organization to foster employee choice and empowerment.

These are good things, but a healthcare organization has larger concerns. Security as it relates to information that must remain private is key among those concerns, but so is the worry that someone who brings their own phone will be more likely to be distracted during the course of the workday. They may be more likely to talk with friends or check social media on their own phone.

Especially in hospital environments, where staff awareness must remain high and immediate reaction to incidents is critical, these potentially negative aspects of BYOD can be enough to scare an organization away from the approach entirely.

This is all about control. It is about how, through new technologies, the healthcare organization can ensure that information is protected, that employees are using the devices appropriately for work purposes and that all policies are being enforced.

Consider this scenario: An orthopedic unit nurse starts work at 7 a.m. Upon clocking in, the nurse's Android phone – which the nurse owns but also uses on the job – becomes activated as a work device. It can be programmed by the IT department to be usable only for work-related activities – with no way to call friends or access social media – except for strictly defined work breaks and lunch or dinner periods.

The device is connected to the internal hospital communications network and assigned a dedicated phone number or extension for use with patients and staff. At the end of the shift, the mobile phone is programmed to switch back to an entirely personal device; the on-the-job "persona" won't appear again until the nurse is back on the job.

Installing a dual identity on the phone, with all policies concerning the work-related identity set by the IT department, ensures that these policies cannot be circumvented.

For example, the nurse may have had access on the job to private patient information on the phone, but that access is blocked when off the job. At that point, it becomes the nurse's personal phone again.

In addition to guaranteeing security and privacy, the use of BYOD phones with tightly controlled usage policies also can save a hospital or other healthcare organization money.

Today, many such organizations invest heavily in blanketing a campus with voice-grade Wi-Fi equipment for communications throughout their facilities. Essentially, these organizations have become wireless service providers. They may not charge users for providing that service the way public mobile carriers do, but they are setting up and continuously managing the service infrastructure and bearing the capital and operating costs associated with it.

By employing BYOD mobile devices as part of an overall communications strategy, healthcare organizations can take advantage of the networks already established by the major mobile carriers. They may need some equipment to assure coverage in particular areas of their facilities, but not to the extent that is needed to create their own networks. In this kind of environment, typically the number of expensive desk phones can also be significantly reduced or even eliminated in favor of an all-mobile approach.

> By employing BYOD mobile devices as part of an overall communications strategy, healthcare organizations can take advantage of the networks already established by the major mobile carriers.

The same mechanism that creates and distinguishes between the work and personal identities can also be used to implement productivity-enhancing capabilities that improve patient care. Integrating BYOD mobile devices with the hospital communications systems can enable an on-duty nurse to be alerted by a patient or staff through the hospital's existing paging systems.

In addition, all calls to and from that mobile phone can take advantage of a single number – a dedicated hospital number or specific extension. One issue with BYOD in any organization is that the number associated with the employee's mobile phone may show up on business calls, which can be confusing to customers and co-workers. By integrating the mobile phone with the hospital's communications network and with a dedicated work phone number or extension, the worker's mobile phone essentially becomes their work phone no matter where they are on the job. Such a solution can enable doctors to call back patients displaying the doctor's office number rather than their personal mobile number, even when the doctor is away from the hospital.

> As with so many organizations today, healthcare has become more mobile than ever before. Taking advantage of the capabilities of employees' own phones – while assuring security and confidentiality while reducing costs – is something that more and more healthcare organizations are embracing.

In addition, all features of the hospital's existing communications system can be extended to the mobile phone. That includes conference calling, short-code dialing, a single voice mailbox, call screening, and other advantages. One university hospital in Canada is doing this, particularly taking advantage of two features. Those features are short-code dialing for employee convenience and simultaneous ringing at both the desk and mobile phone, so a staff member can easily be reached anywhere in the facility.

Finally, the mobile phone can also be used in environments where regulations or organizational preferences require the calls to be recorded. In this case, the mobile phone calls and messages can be recorded through the same systems used to record desk phones or other communications devices.

The partnership between BlackBerry and Tango Networks addresses the expanding importance of healthcare regulatory compliance, specifically call recording. Some healthcare organizations already require a regulatory compliant call recording platform for desk devices, but few have tied the call recording platform in the mobile device.

By combining BES and the Tango Networks Mobile Call Recording application, all calls to and from any mobile device, including iOS, Android, Windows Phone and BlackBerry smartphones, can be recorded based on rules defined by the organization. These rules cannot be circumvented by the end user and are assured to be regulatory compliant.

Beyond regulatory compliance, the BES/Tango Networks Mobile UC application pairing can be used to provide complete administrative and mobile policy control of corporate liable mobile devices. The BES can be used to enforce use of the Business Line on the mobile phone such that all calls are managed and controlled by the Tango Networks platform.

As with so many organizations today, healthcare has become more mobile than ever before. Taking advantage of the capabilities of employees' own phones – while assuring security and confidentiality while reducing costs – is something that more and more healthcare organizations are embracing.

Andrew Silver is Chief Technology Officer for Tango Networks (tango-networks.com), an enterprise mobility solutions provider and BlackBerry partner.

University Health System uses BBM Protected, BES10 and More to Help Improve Patient Care

Industry:
Healthcare

Region:
EMEA

Solution:
BlackBerry® Enterprise Service 10 (BES10), BlackBerry® 10 smartphones, BBM® Protected

Aneurin Bevan University Health Board (ABUHB) in the United Kingdom employs more than 13,000 staff members, two-thirds of which are involved in direct patient care. Consultants, doctors, nurses, midwives, allied professionals and community workers cover the areas of Blaenau Gwent, Caerphilly, Monmouthshire, Newport, Torfaen and South Powys to serve an estimated population of more than 639,000 residents.

GIG CYMRU NHS WALES | Bwrdd Iechyd Aneurin Bevan Health Board

The Challenge:

ABUHB's serves one-fifth of the Welsh population in both hospital and in-home settings. The healthcare providers needed a way to communicate quickly and efficiently among staff to better coordinate patient care.

"Our staff deals with everything from routine medical care to emergency situations. It's imperative that we can contact each other at a moment's notice for general queries, shift changes or weather emergencies," explained Karen Newman, head of Communication, Aneurin Bevan University Health Board. "Yet in our line of work, staff is rarely in an office to manage cases from their computer. We lose a lot of time when staff has to drive back and forth to complete paperwork or attend meetings."

With medical histories and confidential patient information, security was another big concern for ABUHB.

"When nurses are in the field they need a secure channel for communications and access to the records they need to perform their jobs safely," said Drew Evans, head of Information and Communications Technology, Aneurin Bevan University Health Board.

There were also budgetary concerns about implementing a new mobility solution. "We are always being asked to do more with less," added Evans. "We needed a flexible solution that wouldn't eat up all of our IT resources to deploy and manage."

> BES10 also provides one simple management interface that enables us to administer a number of different devices out in the field whether they're on Android, iOS or BlackBerry devices.
>
> **Drew Evans, head of Information and Communications Technology, ABUHB**

The Solution:

New BlackBerry 10 smartphones were issued to employees, and ABUHB upgraded its BlackBerry® Enterprise Server 5 to BlackBerry Enterprise Service 10 for its Enterprise Mobility Management (EMM) solution. ABUHB chose BES®10 for its ability to securely manage other devices as they wanted to implement Bring Your Own Device (BYOD) and Corporate Owned, Personally Enabled (COPE) policies.

"We already had an extensive BlackBerry infrastructure internally, so upgrading to BES10 allowed us to leverage our existing EMM and slowly migrate devices instead of doing the entire company at once," said Evans. "BES10 also provides one simple management interface that enables us to administer a number of different devices out in the field, whether they're on Android, iOS or BlackBerry devices."

BBM® has also enhanced communications among staff. "We've created BBM groups around the on-call schedule, which users can access from a BlackBerry smartphone, Android or iPhone. If a nurse needs someone to cover her shift, she can send a message to the group and everyone can see the responses," said Newman. "This helps supervisors better manage over time and know who to assign cases to."

ABUHB has realized cost savings from its BlackBerry EMM solution. "We've found BES10 meets our budget requirements with a low total cost of ownership. We only need one EMM to manage all of the devices in our network even though we have BYOD and COPE policies," explained Evans. "BES10 only requires a small team to manage it, and the training requirements are minimal. We also like that when issues arise, we can provide technical support remotely through a Web interface."

The cost savings haven't come at the expense of security. "BlackBerry's encryption technology ensures our data is safe and secure – from emails to documents to pulling down data from the cloud when we're in the field," said Evans. "If a device is lost or stolen, we can wipe it clean without worrying that patient confidentiality has been compromised."

ABUHB has also been doing a pilot test of BBM® Protected, which adds a layer of additional encryption to BBM messages between employees while allowing them to use the same BBM app to message family and friends. "We have been running the pilot of BBM Protected for several weeks now and are pleased with how seamless of an experience it has been for our end users," said Evans. "Because we deal with sensitive data, security and privacy are a foremost concern. BBM Protected allows us to adopt an even greater level of security without losing the immediacy and flexibility that our employees enjoy by using BBM."

ABUHB's Benefits:

Many of ABUHB's staff members have begun using their BlackBerry 10 smartphones in place of their laptops to perform daily tasks. "The strength of the integration with Microsoft® Office is really remarkable – stronger than any other device I've used," said Evans. "With the five-inch screen of the Z30 and document editing capabilities it's really easy to use my BlackBerry for Microsoft programs like Word® and Excel®. For me it's faster to type on my BlackBerry because the technology recognizes the words I commonly use and they pop up on the screen. All I have to do is flick them up into the sentence I'm writing."

The ease of using the BlackBerry smartphones, and their productivity-enhancing apps, has made it easier for ABUHB employees to focus on patient care. "When our nurses are mobile and making home visits, it frees up hospital beds for patients who require more intensive care and monitoring. Our secure EMM solution makes it possible for nurses to access the records they need to perform their job and serve patients from the comfort of their homes."

Overall, employees have been very satisfied with the user experience of the BlackBerry 10. "The Hub makes it so easy to view all your emails, messages, texts, calendar appointments, etc., at a glance," said Newman. "Plus, with BlackBerry Balance technology I have separate work and personal spaces. I no longer need to carry around two phones in order to check my personal email or browse the Web. The battery life holds up impressively well – I can use it regularly throughout the day without worrying where the next outlet will be."

Key Benefits

- Seamless integration with key business applications
- More focus on patient care
- Increased productivity
- Enhanced security for patient records

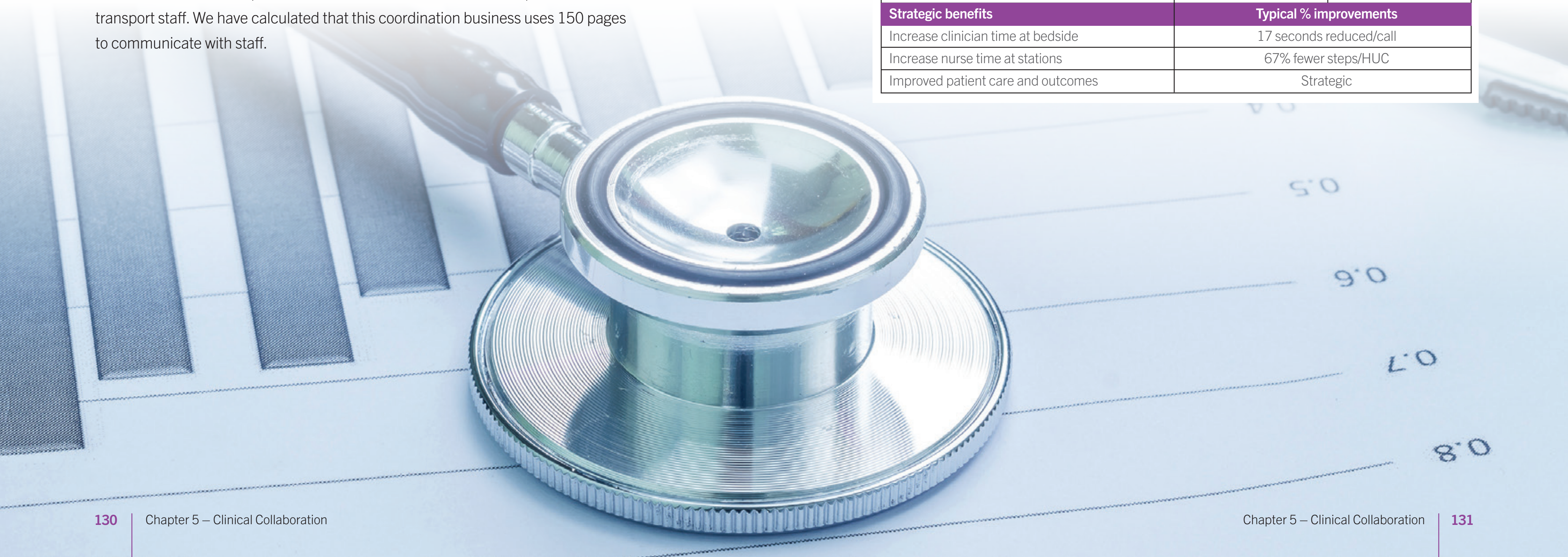
TCO of Clinical Collaboration

The BlackBerry TCO calculator for clinical collaboration provides healthcare organizations with a way to calculate the productivity and strategic benefits of implementing mobility to manage care coordination and patient engagement both inside and outside care facilities. Even incremental timing improvements for shift changes among nursing and telemetry (medical device) monitoring staff, or response time for a telemetry alert, for example, can create big savings for such organizations. The TCO calculator examines the cost implications of certain common coordination activities and shows administrators how even very modest improvements in these areas can add up to substantial business and cost benefits.

The calculator uses data drawn from an actual case study. For the purposes of this calculator we are using an organization with a staff size of 250 people, of whom 100 are nurses, 100 are Health Unit Coordinators (HUCs), and 20 are transport staff. We have calculated that this coordination business uses 150 pages to communicate with staff.

Table 1

Recurring benefits	Conservative estimate	Most likely cost
Overall recurring benefits	$1,205,958	$1,808,729
Quantified benefits	**Conservative estimate**	**Most likely cost**
Shift change – Telemetry	$18,068	$22,995
Per telemetry alert – Telemetry	$33,000	$60,667
Shift change – Nursing	$54,750	$91,250
Per telemetry alert – Nursing	$54,750	$91,250
Transport staff	$122,640	$154,760
Annual pager cost savings	$327,953	$382,703
Productivity savings	**Conservative estimate**	**Most likely cost**
Productivity savings totals	$594,798	$1,005,105
Time spent looking for phone/person – Nurse	$486,667	$811,111
Time waiting for page – Nurse	$30,417	$91,250
Time spent looking for nursing staff – HUC	$55,891	$73,081
Time spent on finding house phone – Transporters	$21,824	$29,662
Strategic benefits	**Typical % improvements**	
Increase clinician time at bedside	17 seconds reduced/call	
Increase nurse time at stations	67% fewer steps/HUC	
Improved patient care and outcomes	Strategic	



The following table shows that our example organization can expect a recurring $33,000 and $61,000 benefit by improving telemetry alert response times. To arrive at the numbers we estimated that the organization cut the time to respond by about 1.5 minutes per alert by implementing mobile technology (see Table 2).

Table 2

Per Telemetry Alert	Conservative estimate	Most likely cost
Time Taken / Alert (minutes)	1.5	2
No. of alerts/year	120,000	130,000
Hourly rate	$11.00	$14.00
Annual Cost	$33,000	$60,667

In Table 2, we can see that the organization handles roughly 120,000 telemetry alerts each year meaning it potentially saves 180,000 minutes (1.5 X 120,000) or 3,000 hours in total response times. If we assume a low-end hourly rate of $11 per hour for telemetry response staff, the organization can save up to $33,000 conservatively (11X 3,000).

If we assume a common hourly rate of $14 per hour, the same organization saves $60,677 per year. The specific numbers will vary by organization. For example, your coordination business might receive less than 120,000 alerts per year or lot more, or your hourly rate for staff could be different from the sample numbers. In either case, replacing the sample numbers with your own will provide a more accurate estimate for your specific situation.

You can similarly analyze other activities that are impacted by mobile technologies. For example, by automating the nursing shift management process, healthcare coordination firms can reduce costs by between $55,000 and $91,250. To arrive at the number, we considered the time taken (in minutes) to manage the shift (1.5 percent), the number of registered nurses (100), their hourly rate, and costs per day (see Table 3).

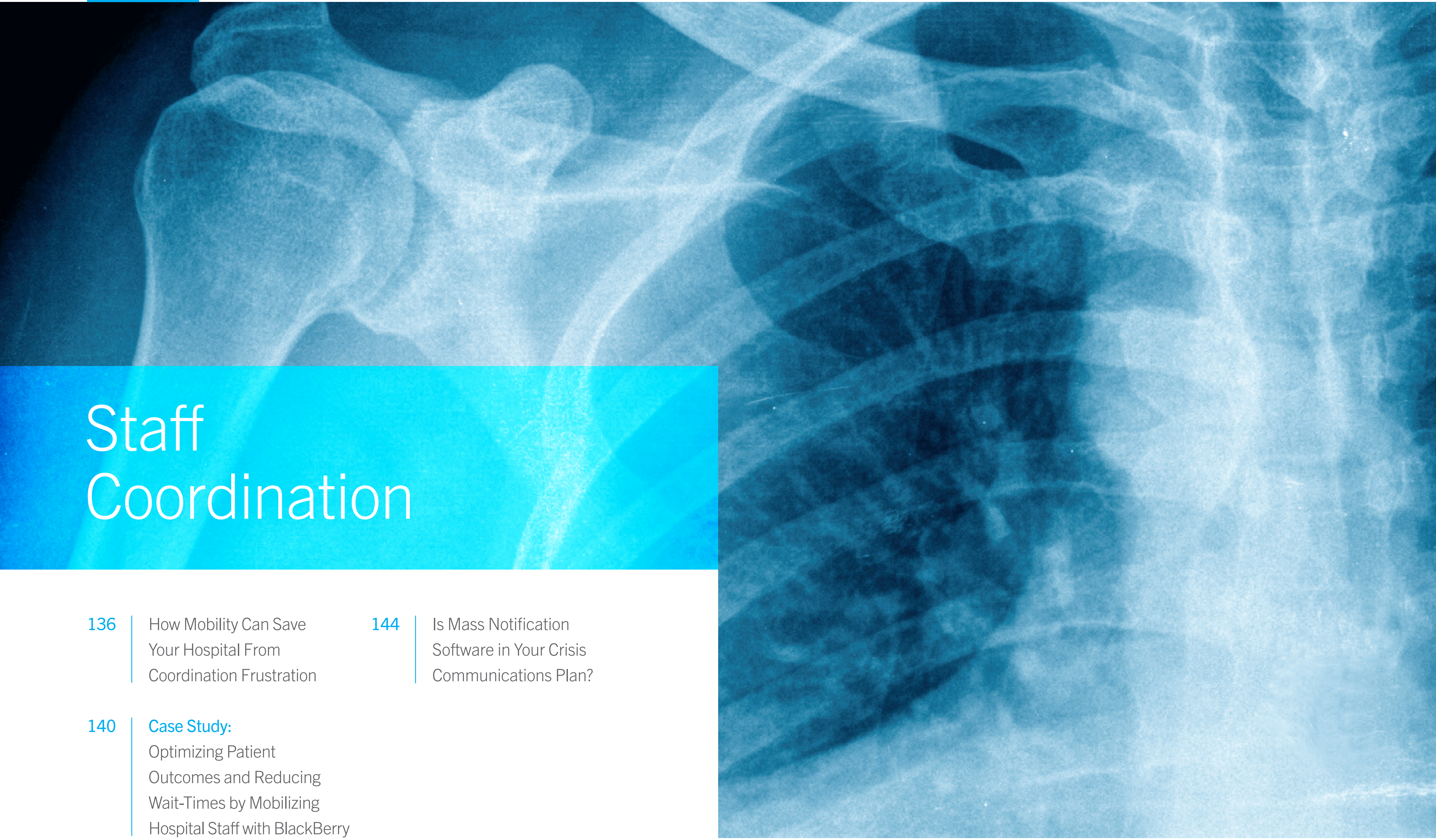
Table 3

Shift Change – Nursing	Conservative estimate	Most likely cost
Time Taken (minutes)	1.5	2
No. of times/day	3	3
No of Registered Nurses	100	100
Hourly rate	$20.00	$25.00
Cost per day	$150	$250
Annual Cost	$54,750	$91,250

To evaluate the impact on shift change, we multiplied the time taken for a shift change, with the number of shifts per day and the total number of registered nurses in the organization. The final cost savings per day worked out to $150 per day or about $54,750 on an annualized basis conservatively and $91,250 at the higher end.

In our example, the business stands to save between $1.3 and $1.8 million on an annual recurring basis as a result of implementing or improving mobile technology. The savings come from improved efficiencies across multiple activity areas including shift changes, response times to alerts, and reducing the overall number of pagers necessary for the business.

Chapter 6



Staff Coordination

How Mobility Can Save Your Hospital From Coordination Frustration

By Sarah Padfield, Chief Operating Officer, Chatham-Kent Health Alliance

In a perfect world, every hospital would be a well-oiled machine. Employees would always be where they were needed, expensive equipment would never sit idle, and patients would never have to wait. Unfortunately, we don't live in a perfect world, at least not yet.

Hospitals tend to be chaotic, confusing places for employees as well as patients. Housekeepers and transporters are under constant pressure from doctors and nurses, who in turn must deal with upset patients and their families. Throw confusing scheduling or missed communications into the mix, and it makes for a frustrating workplace that can hurt patients, employee morale and the hospital's bottom line.

Can I Get A Bed?

Consider the following scenario: a patient is waiting in the ER to be admitted. The only way for the admissions desk to find out when a room will be available is to ask housekeeping. A housekeeper reports to the nurses' station to get more details, maybe waiting in line to talk to someone. Then the housekeeping staff must determine room availability by calling or paging around or even relying on word of mouth. In the meantime, the nurse working in the ER must calm an increasingly frustrated patient. The nurse lashes out at housekeeping, asking why no rooms are available. Why aren't they doing their job?

> By automating employee workflow with smartphones and apps, hospitals can make both support personnel and patients a lot happier.

Multiply this situation a few times over and the waiting room becomes overcrowded. Patients in need of a bed have lengthy wait times while others are turned away or transferred to other facilities. In addition to lost revenue from transfers, long wait times cause the hospital to miss out on a number of financial incentives.

The Underutilized Operating Room

Poor coordination doesn't hurt just admissions, of course. Let's look at it how it affects a couple of other areas.

Without proper coordination, transporters can fail to deliver patients to surgery on time. This forces expensive hospital space and equipment to sit unused. Surgeries may also have to be cancelled if patients aren't able to be admitted into a bed. This may mean operating rooms sit unused – this is a serious problem.

Finally, a harried staff is often an unhappy one. In a 2001 study, the *Ontario Hospital Association* found that support workers are among the least satisfied of hospital employees and have a higher turnover rate than even registered nurses.

Fortunately, hospitals already have it within their power to fix many of the problems associated with poor staff coordination.

By equipping support staff with the right set of mobile applications, hospitals can automate workflow, increase employee satisfaction, and improve both outcomes and income.

Consider how the previous scenario might play out if housekeeping were equipped with a mobile coordination platform.

A patient waiting in the ER is ready to be moved into a room. A housekeeper receives an alert on their smartphone that a task is waiting, which they can either accept or reject. If they accept, they can view relevant instructions, such as droplet precautions and other proper cleaning measures. If they're busy and reject the task, the request is automatically sent to the next available housekeeper.

When the room is clean, the housekeeper pulls out their phone, opens the app and clicks Finished, sending an alert that the room is ready. The admissions department quickly moves the new patient into the room. The process is quick and painless for everyone, and most importantly, transparent so everyone in the organization can see the data, processes and bed status across the hospital.

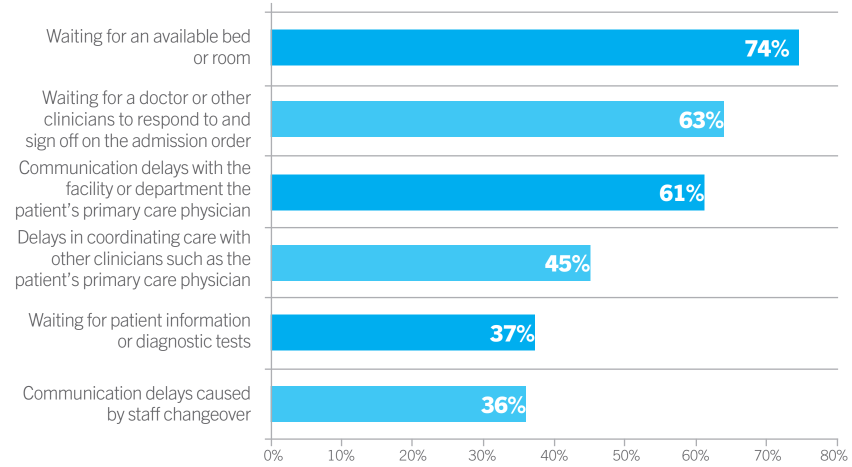
Mobile's Ripple Effect

As you can see, mobilizing just one area not only increases the efficiency of that department but sends a positive ripple across the hospital. By sending alerts and reporting through a mobile platform, hospitals can keep staff updated and provided with all the information they need to do their jobs.

Here's what you can expect to gain from equipping your staff with smartphones and mobile apps:

- **Faster admissions.** In the example we gave, our hospital, Chatham-Kent Health Alliance, was able to reduce patient wait times for admission by 50 percent by equipping our housekeeping staff with Oculys KeepNTouch on BlackBerry smartphones.
- **Reduced disease outbreaks.** By equipping employees with a tool that provides on-the-spot instructions and best practices, hospitals can ensure that staff follows proper cleaning and disinfection procedures.
- **Better communications.** Rather than having to communicate through a series of pages or physically hunting down staff, teams can contact one another directly through their smartphones.
- **More equipment uptime.** Because staff will be where they need to be when they need to be, equipment and operating room downtime will decrease.
- **Better relationships among employees.** More efficient operations improve morale and make work a less stressful, happier place to be, people get recognized for the collective effort in improving performance across the organization.

The main reasons for inefficient communication during the patient admission process



Source: Ponemon Institute Research Report 2014

> A lack of coordination in hospitals is one of the healthcare industry's most vexing problems.

A lack of coordination in hospitals is one of the healthcare industry's most enduring problems. By simply tapping into the power of mobile technology, hospitals can help their employees work more efficiently, effectively, and successfully. That means a more perfect world for both patients and hospitals.

Sarah Padfield is Chief Operating Officer at Chatham-Kent Health Alliance and is a certified member of the Canadian College of Health Leaders.

CASE STUDY

Optimizing Patient Outcomes and Reducing Wait-Times by Mobilizing Hospital Staff with BlackBerry

Industry:
Healthcare

Region:
North America

Company Size:
Medium

Solution:
BlackBerry® 10 smartphones, BES, Oculys Performance, Oculys KeepNTouch

Chatham-Kent Health Alliance (CKHA) is a 200-bed community hospital equipped with state-of-the-art facilities and technologies that sees over 65,000 emergency room visits per year. Formed in 1998, CKHA is committed to core service excellence, top-flight operational performance and to being the facility of choice in the region. CKHA also serves as a teaching facility for the Schulich School of Medicine and Dentistry.

The Challenge:

Efficient patient flow is critical in any hospital environment. It is especially important to minimize the time for a patient waiting in the Emergency Room (ER) to be admitted. Negative patient outcomes, such as the risk of deterioration, increase the longer a patient has to wait for a bed. For CKHA, the first step to improve patient flow was to provide better visibility for all their staff into what was happening across all areas of the organization.

"We would call admitting and be able to gather some information and then we'd be on the phone with the ER for other information. We would often be physically walking around to gather all of the information we needed to really understand what was happening in the hospital," said Sarah Padfield, Chief Operating Officer at CKHA. "We were really good at knowing what happened yesterday, but were having a harder time predicting what today would be like."

The next objective was to find a way to move patients out of the ER and into a bed more quickly. To achieve this objective, CKHA wanted to find a way to make it easier for the housekeeping staff to communicate to the rest of the healthcare team that rooms were clean and beds were prepared to accept new patients.

Key Benefits

- Reduced patient admission wait times by 50 percent
- Streamlined workflow for housekeeping staff
- Improved patient satisfaction
- Improved patient outcomes

Source: CKHA

"In the past, we didn't necessarily know when a bed would be available and ready in a timely manner. Patients were left waiting for an extended period of time in the ER," said Padfield. "We didn't have a clear idea of what was happening in housekeeping. It was something so simple, but we knew that we had to do something to make that part of the patient flow work more efficiently."

The Solution:

CKHA wanted a simple way to provide visibility into what was happening in the hospital. They engaged with Oculys, a healthcare technology company focused on delivering real-time, integrated support solutions designed for healthcare organizations. CKHA deployed a software solution called Oculys Performance to give all staff members a big picture view into the flow of patients throughout the hospital.

Since the staff at CKHA was already using BlackBerry® 10 smartphones, Oculys Performance is easily accessed by staff members via a web-based application no matter where they happen to be. "With one look, our staff can see the number of patients currently waiting in the ER and intensive care unit, compared to beds available," Padfield said. "Oculys Performance tells me how many people are ready to be discharged or who requires alternative care. I can see same-day visits or surgery patients that require admission. It's an all-in-one, simple-to-view dashboard. And, since I'm usually on the go, I rely on my BlackBerry to get to all the information wherever I am."

CKHA then worked with Oculys on another solution, this time for their housekeeping staff. The hospital discovered that the housekeeping staff was already using personal BlackBerry smartphones to communicate with one another via a BBM® group. Since the hospital was mindful of security issues, they elected to give the housekeeping staff corporate issued BlackBerry 10 smartphones, managed by BES.

Deploying BlackBerry smartphones with Oculys KeepNTouch, a housekeeping application, put a powerful tool in the hands of the staff that are at the front line of care. The Oculys KeepNTouch application is simple to use; staff can see which rooms they are assigned, and click a 'start' button when they enter the room, which triggers a timer to measure how long it takes to clean each room. Once the room has been cleaned, they press an 'end' button and a notification is sent back to the central admitting department that the room is ready. There are also special instructions embedded in the application. "If there are exceptional circumstances required for a specific situation, such as cleaning a room where the patient was in isolation, the application guides the staff with checklists that apply to that particular situation," said Padfield. "This is especially important for the safety of our staff and to reduce the spread of infection."

Chatham-Kent Health Alliance's Benefits:

Since deploying the Oculys solution on BlackBerry smartphones, CKHA has seen tremendous reduction in wait times for patients requiring admission. Prior to implementing the Oculys solution, the average patient wait time in the ER for patients between the time an admission was started to the time they got a bed was between 18 and 20 hours. Now, this average wait time is approximately 8-10 hours. This makes for a 50 percent reduction in wait times.

"Since implementing the Oculys solution on BlackBerry, our Ontario provincial ranking has improved significantly. We are now 6th in the province for patient admission wait times, versus 16th prior to implementing the solution. That's not only impressive to us, but we're finding that our patients are happier that they are being treated more quickly," said Padfield. Since risk of deterioration increases the longer patients have to wait in the ER, CKHA can also correlate an improvement in patient outcomes based on shorter wait-times.

> Oculys KeepNTouch on BlackBerry is helping our housekeeping staff to be more efficient and has streamlined their workflow. Our admitting department has a real-time notification that a bed is clean and ready for the next patient. It's incredible what a seemingly simple solution has done to help us shorten patient admission wait times, and ultimately improve our patient outcomes.
>
> **Sarah Padfield, Chief Operating Officer, Chatham-Kent Health Alliance**

The housekeeping application has improved communications between housekeeping and management and has reduced wasted time and energy in locating staff and assigning tasks. It has also been empowering for the housekeeping staff themselves. "This project has created a real sense of pride within our team because it showcases that we are a progressive group who can see the benefits that technology will bring to our work," said Carrie Sophonow, Housekeeping Manager CKHA. "Since implementing this solution, we are seeing increased efficiencies and new opportunities for our team to make a positive impact for patients at CKHA."

"Oculys KeepNTouch on BlackBerry is helping our housekeeping staff to be more efficient and has streamlined their workflow. Our admitting department has a real-time notification that a bed is clean and ready for the next patient," Padfield explained. "It's incredible what a seemingly simple solution has done to help us shorten patient admission wait times, and ultimately improve our patient outcomes."

Is Mass Notification Software in Your Crisis Communications Plan?

By Guy Miasnik, President, AtHoc, a Division of BlackBerry

A patient pulls a gun on a nurse and demands narcotics. A tornado hits a nearby facility and you need to check on the well-being – and availability – of off-duty staff. A five-alarm fire has engulfed the block next to your downtown clinic. A field-based healthcare worker is taken hostage in the home of a mentally ill client. Would you know how to keep everyone on your staff safe and informed during any one of these calamities?

Hospitals care for society's most vulnerable: the newborn, the injured, the sick. During emergencies hospitals help hold communities together, so it's vital to everyone that healthcare workers themselves stay safe during crisis situations.

A good crisis communications plan is essential in order to be ready for the next emergency that could threaten your hospital staff's physical safety or ability to take care of patients. A plan set down on paper is a good start but not enough. You need a system-wide network tool that will alert every staff member and provide instructions on what to do next.

The best mass notification systems are capable of sending alerts to all the devices people use, plus PA systems, sirens, and other equipment if the situation warrants it. Systems should be flexible enough to function well in any crisis, from violent patients to severe weather to a flu epidemic, and they should offer secure two-way communications so those alerted can report back and be accounted for.

AtHoc, a division of BlackBerry and a Leader in Gartner's Magic Quadrant for Emergency Mass Notification Services, created crisis communication software that offers all these features. The U.S. Department of Veterans Affairs and their large network of healthcare facilities, along with Kaiser Permanente and many other high-profile organizations, are AtHoc clients, but these systems are deployable by institutions of any size.

Vulnerable Healthcare Workers

Experts tell us violence is a serious personal safety problem healthcare workers face. U.S. healthcare employees miss work due to work-related violence four times as often as private industry employees, according to the Bureau of Labor Statistics. More than 2,300 threats or acts of violence were reported between January and July of 2014, with the consensus that many more incidents go unreported, according to the Red Cross.

When violence occurs, every second counts. According to the FBI, the typical attack by a lone gunman lasts about 12 minutes. With the average 100-bed hospital employing as many as 850 staff members, hundreds of people might be on duty when an attack occurs. In a healthcare facility, every minute of delay greatly increases the risk of harm, not only to employees but vulnerable patients.

Since most employees carry phones, someone might be able to call security or 911 during an attack. However, these kinds of alerts are hit-or-miss at best. Law enforcement often doesn't know what to expect when they arrive. More importantly, there is no easy way to give other employees in the building instructions that could save their lives, such as to stay hidden, or to avoid certain parts of the hospital.

A network-wide system lets a hospital alert everyone in the safest way possible, such as smartphone texts or desktop popups. In fact, the Occupational Health and Safety Administration (OHSA) recommends that businesses use alarms, radios, cell phones and other security devices as part of an emergency response system.

> "With the average 100-bed hospital employing as many as 850 staff members, hundreds of people might be on duty if an attack occurs."

Anatomy Of A Crisis

Here's how AtHoc might protect staff in one fictional situation. It's early evening during a shift change when hospital employees hear a series of loud pops. A nurse who has taken cover in a bathroom calls the front desk, who tells a manager that a gunman is stalking the second floor of the eight-floor building. The manager uses the AtHoc system to quickly compose a message detailing everything she knows about the situation and chooses the distribution list for the entire hospital, including off-duty employees.

Her distribution list includes notifications to the network of community organizations she set up to contact in emergencies, including the police and fire departments. She includes a couple of response choices ("I'm okay," or "I need help"), selects the devices she wants the alert to go to – desktop, mobile phone, work phone, home phone, even social media, but not the hospital PA system -- and hits Publish. Quickly and with one click she has alerted not only every hospital employee but also the local authorities. The AtHoc system collects responses as they come in and she or other emergency managers can view them aggregated or drill down to specific employees if necessary so authorities know where to concentrate their rescue efforts.

Clinical Outages

Not all emergencies come from outside events. With AtHoc's crisis communication software, managers can reduce downtime from disabled servers or applications and keep patient care continual.

For instance, the IT department becomes aware the network can't access medical records. An IT manager uses the AtHoc system to send an alert to all affected parties in the form of a popup window on each clinical workstation. When users click on an acknowledgement button they are redirected to an alternate means of accessing critical information. Through alerts to desktops and smartphones, IT can keep you in the loop about progress, including final resolution.

> The Department of Veterans Affairs uses AtHoc to protect 500,000 personnel in its medical centers and outpatient, community, and outreach clinics across the nation.

Preparation Saves Lives

AtHoc alerts have helped keep personnel safe in several tragedies over the years, including shootings at the Washington Navy Yard, Fort Bliss and Fort Hood. The Department of Veterans Affairs uses AtHoc to protect 500,000 personnel in its medical centers and outpatient, community, and outreach clinics across the nation. Every clinic, physician, nurse and technician in Kaiser Permanente's AtHoc system is notified in a crisis situation. Twenty-one hospitals are able to send two-way alerts, and manage shift changes and scheduling through automated staff messages.

Other AtHoc customers include the U.S. Departments of Defense and Homeland Security, U.S. Department of the Treasury, and AtHoc safeguards numerous other government agencies and leading commercial enterprises including the Red Cross, the University of California, Eastman Chemical and the U.S. Coast Guard.

If you've been meaning to beef up your crisis communications plan, now is always a good time. Your employees are depending on you.

Guy Miasnik is President of the AtHoc division of BlackBerry. He co-founded and was CEO for AtHoc, which helps safeguard millions of people in thousands of organizations worldwide in commercial, healthcare and government enterprises.

Home Care

Why Home Healthcare Should Go Mobile

By John Schram, former President and CEO, We Care Home Health Services

Healthcare continues to undergo a transition, one driven by an aging population, chronic diseases and rising costs. Where once an elderly patient might have spent weeks recovering completely in a hospital bed, now she's encouraged to find an alternate care level (ACL); in other words, an arrangement in which she can safely complete her convalescence that's less expensive for all concerned, patient and provider alike.

That's where home care services come in. Hospitalization is not only expensive, it can be stressful for patients and actually slow down their recovery. Often, discharge is a better choice, but only if the patient has a safe place to go. Home care is increasingly providing support for these patients. Workers who come to the patient's home can provide full monitoring and support and often save patients with mobility challenges the trouble of repeated doctor visits for follow-up care. The same services can assist seniors in their daily lives, allowing them to "age in place" where they are most comfortable – their home.

Home Care's Challenges

The home care sector is growing. Market research firm *Tractica* estimates that the number of patients worldwide using some form of home health technology will increase from 14.3 million in 2014 to 78.5 million by 2020. The benefits are clear. Patients treated at home remain closer to family and friends and get one-on-one care that tends to be more personalized than the hospital experience. These advantages lead to happier patients and faster recoveries.

Though home care offers many benefits, it is not without its challenges. For one, there is a lack of consistent, uniform standards for the industry. Although some home care agencies are accredited by authorized authorities, such as Accreditation Canada, ensuring standard practices and providing programs for continuous quality improvement.

Lack of communication can also be a serious problem. Home care workers work on their own and may not have immediate access to their supervisors or a back-up clinician. If they see something they don't know how to deal with while tending to a patient in the field, they're largely on their own with no easy access to advice.

Another hurdle is recordkeeping. According to *VDC, a market researcher based in Natick, Mass.*, "20-25 percent of service providers' time is spent on administration, placing a significant financial burden on home care service providers." Tracking of employees' time and the ability to deal with cancellations and missed visits are also difficult.

The above factors may lead to a poor patient experience and contribute to high annual turnover among home care workers, with rates as high as 62 percent, according to a 2014 survey by *Home Care Pulse conducted in the US*.

Lastly, for some jurisdictions, there is the matter of regulatory compliance. By law, patient data must be adequately protected and secured; failure to do so will result in financial penalties, reputational damage and possibly litigation.

> "Home care workers work on their own and may not have immediate access to their supervisors or a back-up clinician. If they see something in the field they don't know how to deal with, they're on their own."

> The number of people worldwide seeking home health care will more than quintuple to 78.5 million by 2020.

Automated Reporting To The Rescue

Mobile technology from BlackBerry and their partners helps address the home health care challenges in the following ways:

- **Real-time, secure access to patient data.** To ensure continuity of care, home care providers must have a patient's information and care plan available when they arrive for an appointment. They need to ensure that the patient's data remains private so that they comply with regulatory requirements, and they need access to the data regardless of connectivity.
- **Automated reporting.** Automating the reporting of details such as patient visits and the hours and mileage of care providers considerably reduces administrative overhead.
- **Better communication.** Home care workers who use mobile devices are able to consult more often and more quickly with one another and their supervisors, which results in better care for patients. BBM Protected (BlackBerry's secure messaging application) is one tool that enables secure communications through an easy-to-use messaging interface, allowing real-time consultations between home care workers and agency staff while keeping patient data safe and encrypted.
- **Improved scheduling.** Home care providers can give their employees instant access to their schedules and patient information. This allows them to plan their schedule more efficiently and save time. Mobile communications also let staff quickly verify that workers made the visit and reschedule an appointment if necessary.
- **Safety.** Thanks to GPS tracking, an agency can know exactly where each employee is and can see if an employee has not arrived at their next destination on time, allowing them to look into why. This makes home care safer for both patients and home care workers, as agency staff can check in on any appointment that takes longer than it should.

Mobile applications such as CellTrak, GoldCare, Procura™, and the new end-to-end solution from AlayaCare offer most of the features we just described. They improve communications and mobility, automate patient reports and scheduling, and provide home care staff with direct access to clinical information. Used with BES12, they also help agencies comply with government regulations since BlackBerry's comprehensive Enterprise Mobility Management (EMM) solution ensures patient data is safe whether at rest or in transit.

Safe Digital Home Care

Healthcare continues to be in a period of transition, and home care is at the heart of the change. By caring for people at home, providers can ensure better patient outcomes, lower treatment costs, and offer both patients and staff a better overall experience. And by equipping home care workers with the right technology, providers can offer all of this without compromising patient privacy or the safety of their employees.

John Schram is the former President and CEO of We Care Home Health Services and presently sits on the boards of Wellpoint Health Services, AlayaCare Inc., Aureus Health Services and Accreditation Canada, where he chairs the Finance and Risk Committee.

CASE STUDY

Home Healthcare Provider Increases Scheduling Efficiency and Improves Patient Outcomes using BlackBerry Solution

Industry:
Healthcare

Region:
North America

Solution:
BlackBerry® 10 smartphones,
BES®12,
CellTrak VisitManager™

CarePartners is a leading provider of home healthcare services in communities across Ontario. With a dedicated mobile team of nurses, therapists and personal support workers (PSWs), CarePartners delivers a broad range of expert and cost-effective services ranging from chronic illness management, nutrition, physiotherapy, to personal hygiene and support. These services are all aimed at helping to ensure their clients enjoy the freedom and independence that comes with staying in their own homes.

CarePartners

CellTrak connected with care®

Key Benefits

- Reduction in missed patient visits to less than 0.1 percent
- Anticipated 20 percent reduction in administrative tasks
- Real-time access to patient information and scheduling
- Highly secure platform for protection of patient data and regulatory compliance

The Challenge:

CarePartners provides personal support, nursing and therapy services to 14 Community Care Access Centres (CCAC) across Ontario. CarePartners currently has 4,000 mobile workers who provide services for seniors, people with disabilities, post-operative patients and people who need healthcare services to help them live independently in the community. The workforce at CarePartners is almost completely mobile. As a result, nurses, therapists and PSWs are usually out in the community engaging with patients in their homes.

CarePartners needed to standardize processes to make workflows more efficient, increase visibility into patient care plans in real time, and increase the safety of their mobile staff. “In the past, we would inform our staff of their schedule and provide patient information on their voicemail at the beginning of each week,” said Kelly Baechler, Manager of Organizational Change at CarePartners. “If there were cancellations or missed visits, we wouldn’t know about it until the following week. It was also difficult to track exactly where any staff member was at a given time, which could pose safety issues.”

> We chose BlackBerry and BES12 because of the end-to-end security benefits and high level of management and control it affords us. We need to ensure that the GPS is always on, for example, and need the ability to block certain apps from being installed on the device. We can manage all of this through IT policies on BES12. We also need to be assured that our patient information is protected, and with BES12 we know the data is secure and that we are complying with PIPEDA and HIPAA regulations. This is crucial for us.
>
> **Kelly Baechler, Manager of Organization Change at CarePartners**

The lack of standardized processes meant a heavy lift for back office support workers. Everything had to be completed manually, including scheduling, mileage tracking and reporting, as well as phone calls for scheduling changes. This was inefficient, could be prone to errors and wasn't secure.

The Solution:

A long-time BlackBerry user, CarePartners decided to deploy BlackBerry 10 smartphones equipped with CellTrak VisitManager™ to their mobile workforce. Using the VisitManager™ application, staff are able to log in to see their schedule directly on their BlackBerry smartphones. They can also see pertinent patient information in order to better manage their care plans. The application tracks the start and end time of each appointment, which is automatically sent to the head office. GPS tracking available on the BlackBerry smartphones allows the office to have an accurate location of where the staff are at any given time which not only helps to keep staff safe, but helps to reduce the time spent on back-end administrative tasks, like mileage reporting.

CarePartners also deployed BES12 to manage their fleet of BlackBerry smartphones. "We chose BlackBerry and BES12 because of the end-to-end security benefits and high level of management and control it affords us," Baechler explained. "We need to ensure that the GPS is always on, for example, and need the ability to block certain apps from being installed on the device. We can manage all of this through IT policies on BES. We also need to be assured that our patient information is protected, and with BES12 we know the data is secure and that we are complying with PIPEDA and HIPAA regulations. This is crucial for us."

CarePartners' Benefits:

Instant Access to Schedules and Decrease in Missed Visits

Since deploying the BlackBerry smartphones equipped with CellTrack VisitManager, the staff at CarePartners now has instant access to schedule and patient information and real-time verification of visits. This access to real-time information has proved invaluable in tracking missed visits and has given CarePartners the ability to reschedule appointments quickly. This has contributed to a significant decrease in missed appointments, with missed visits now totalling less than 0.10 percent.

"With the CellTrak application on BlackBerry, we're able to more accurately monitor travel expenses," said Baechler. "The app automatically calculates the distance and time and helps us reimburse our staff faster." With the full rollout of the application we are anticipating a 20 percent reduction in the administrative work required to communicate schedules, schedule changes and filling shifts.

Real-time Availability of Patient Information Leads to Better Patient Outcomes

"In home healthcare, the patient's information and care plan must be available 100 percent of the time," said Barry Billings, Vice President, CellTrak. "By deploying the CellTrak VisitManager application for BlackBerry 10, CarePartners and their staff are now able to have real-time access to patient information and care documentation tools, regardless of cellular data coverage. The app was built with a store and forward architecture so that data syncs automatically when staff is back in coverage. And because BlackBerry has end-to-end security built in, CarePartners can be confident that the patient data is protected on the device."

"The peace-of-mind that the BlackBerry and CellTrak solution has given us is probably the most notable benefit," Baechler said, sharing the following story. Recently, CarePartners received an urgent call from a CCAC Care Coordinator regarding a patient receiving PSW services for medication reminder. The paramedics had contacted CCAC after receiving a 911 call. Upon responding to the 911 call, paramedics found that the patient had had a stroke. The paramedics needed to administer stroke medication within three hours of a stroke, but couldn't know for sure if the stroke had occurred within the three-hour window. The CarePartners coordinator logged in to the CellTrak application to confirm the timing of the last visit and could confirm the exact time that the PSW left the patient's home. The PSW had left the patient's home an hour and 50 minutes previously so the paramedics could safely administer the meds without hesitation. "It's cases like this that make technology so important to patient care and safety," Baechler said. "Access to real-time information using our BlackBerry solution helps us to know exactly what's happening with our patients and provide continuity of care."

CASE STUDY

Collaborative Approach to Technology Enables Home Care Provider to Improve Communication and Efficiency

Industry:
Healthcare

Region:
North America

Solution:
BES®12,
BlackBerry® 10 smartphones,
MobilityPlus, by GoldCare

Headquartered in Mississauga, Ontario, Canada, Revera opened its first retirement residence in 1961. Today, in addition to operating more than 200 retirement residences, long-term care homes and skilled nursing facilities (US), Revera is also one of North America's leading providers of home health services. With over 30 home health offices across Canada, Revera's dedicated team members touch the lives of more than 25,000 seniors and their families every day.

The Challenge:

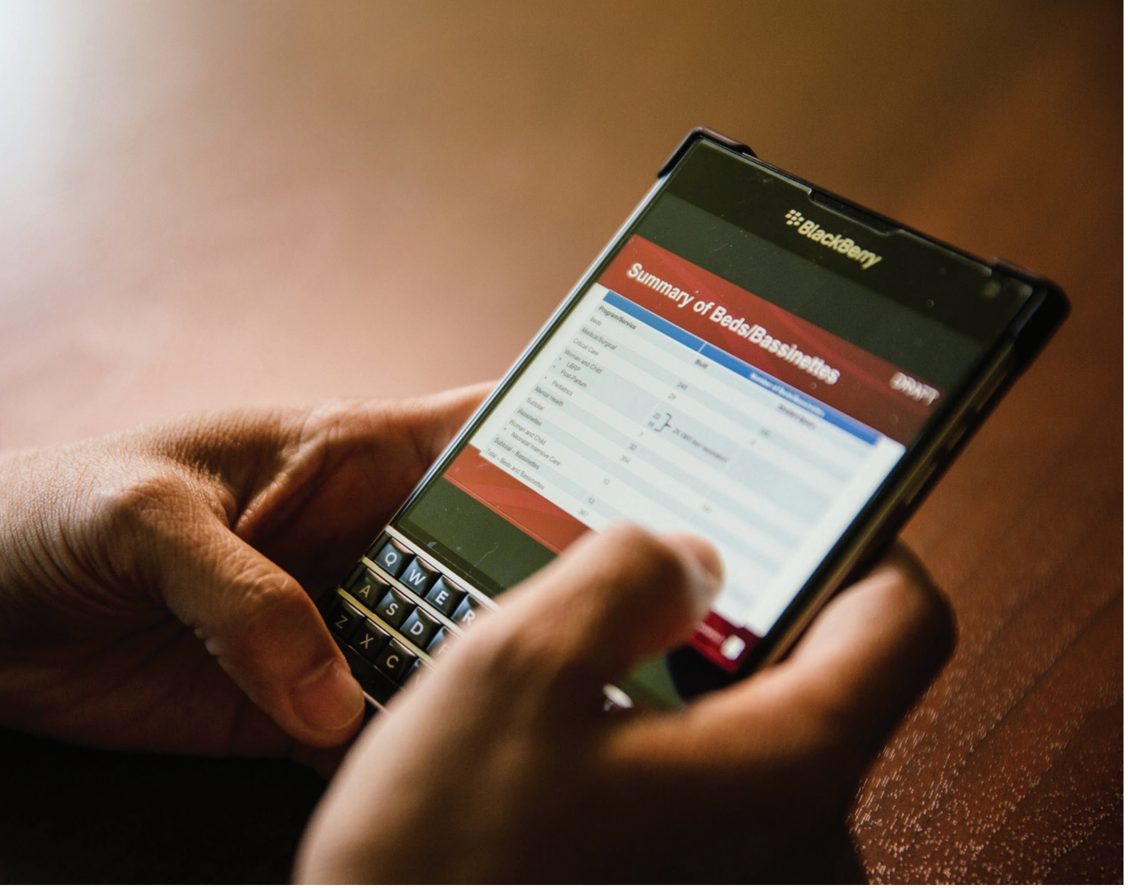
Revera's Home Health division is focused on helping their clients live independently in the comfort and freedom of their own homes – as the company says, they are focused on "helping people live their lives to the fullest." With over 5,000 front line home care staff visiting clients in the comfort of their own home each and every day, Revera required a more effective way to manage scheduling, streamline operational functions and better manage information and information sharing.

Prior to the introduction of BlackBerry solutions, Revera's home care providers relied on a more labor-intensive system to track appointment related client information. Their phone-based system was used to check in once they reached a client's home for their appointment, and again when they left. They would track client data the old fashioned way – through paper copy and were required to keep notes regarding appointment-related information, such as directions to a client's house and necessary contact details. The process was time-consuming and inefficient at times.

Key Benefits

- Improved and secure communication
- Better scheduling, reduced missed visits by 31 percent and improved ability to fill shifts more efficiently
- GPS and geocoding for reduced travel time
- Near real-time check in and check out for appointments
- Improved safety for employees and clients

Revera recognized very quickly that they required a solution that would allow their care providers convenient access to the information they needed, while providing a more integrated approach to log and manage the more than four million hours of services rendered to their clients annually.



> We knew there had to be a better and more effective way to communicate as a team, so we turned to GoldCare and BlackBerry to help us innovate and evolve the mobility strategy of our Home Health division, allowing us to focus on what we do best – providing quality to our clients, in the comfort of their own homes. The decision has resulted in significant enhancements that are having a lasting impact on our business.
>
> **Jo-anne Stone-Burke, National Director, Strategic and Operational Transformation, Revera Home Health**

"We knew there had to be a better and more effective way to communicate as a team," said Jo-anne Stone-Burke, National Director, Strategic and Operational Transformation, Revera Home Health. "So we turned to GoldCare and BlackBerry to help us innovate and evolve the mobility strategy of our Home Health division, allowing us to focus on what we do best – providing quality to our clients, in the comfort of their own homes. The decision has resulted in significant enhancements that are having a lasting impact on our business."

The Solution:

Revera deployed a fleet of BlackBerry 10 smartphones, pre-loaded with GoldCare's MobilityPlus mobile healthcare management application, across its homecare division. Revera also migrated to BES12 as its Enterprise Mobility Management (EMM) platform to securely manage its BlackBerry 10 smartphones as well as the Android™ tablets used by its nurses and therapists.

MobilityPlus is giving Revera's home care providers the freedom to securely manage appointments, as well as client and program information directly on their BlackBerry 10 smartphones. The system has also helped improve documentation, reporting and communication in the field.

The solution is feature-rich with an integrated platform and easy-to-use interface, and ensures that up-to-date client, employee and clinical information can be accessed conveniently and securely.

MobilityPlus allows care providers to access their appointment details and driving routes on their BlackBerry 10 smartphones at the start of each workday. The GPS and geocoding integrated into the application help direct care providers to their next appointment. Care providers can log in to find the best driving route, maps and driving directions, so there's less chance of arriving late or missing an appointment. Care providers can also conveniently dial clients' numbers directly from within the application. In addition, providers have more peace of mind performing tasks knowing that the built-in GPS on their BlackBerry smartphones provides their location in near real time for enhanced lone-worker safety.

Using their BlackBerry 10 smartphone at a client's home, the care provider 'starts' the appointment and then provides the scheduled service. Once all relevant information regarding the appointment has been recorded, the provider 'ends' the appointment. GoldCare then securely transmits the updated information from the smartphone, with location and time stamp, directly to the server-based application in real-time.

GoldCare Chat, which allows for real-time secure messaging between care providers and back office employees, is integrated into the application. Likewise, NotesPlus is integrated, which allows users to record and save detailed notes to the client record, so they're accessible during subsequent visits.

"Once our care providers arrive at a client's home, MobilityPlus allows them to easily document information and better manage the task they are to perform at the client's location. The addition of BlackBerry 10 smartphones to our workforce has helped us realize critical gains in convenient access to information and improved internal communication," said Stone-Burke.

"Together, BlackBerry and GoldCare have helped us improve the way we function as a team and business, opening up an entirely new dimension of secured communication and client data management. This evolution is enabling our employees to provide better services to clients at the point-of-care, resulting in higher quality care and outcomes," added Stone-Burke.

Revera's Benefits:

Since the deployment, Revera has simplified the process for checking in and out at designated appointment locations and the organization now has a centralized system that is better equipped for the management of sensitive client information.

The use of MobilityPlus on BlackBerry 10 smartphones has helped improve communication and collaboration between inbound and outbound employees, and has eliminated the need for multiple streams and disjointed conversations to verify information over home phones, personal cellphones and email.

GoldCare's GPS-enabled solution has also helped providers significantly cut down on travel time, and on late and missed visits, resulting in significant time and cost savings for the organization, while improving the delivery of consistent, high quality care to clients.

"Employees are not just communicating better; they are improving their team dynamics while learning from each other along the way. We are seeing a new level of confidence in our providers, who are feeling more empowered knowing that they have access to the real-time information they need at all times," said Stone-Burke. "Collaborating with GoldCare and BlackBerry has been critical in helping us keep pace with our growing presence in the home care market. We just can't imagine going back to the system that we had before as this new, flexible solution provides us with a solid technology foundation for continuous enhancements to meet our present and future needs."

The next phase of the GoldCare project will include Broadcast Scheduling, which will broadcast messages regarding unscheduled appointments to a broader user base and allow care providers to respond "yes" to the appointment. The system will then automatically schedule that employee to the appointment. Furthermore, a skills match feature will better match a worker's skillset to the needs of a client.

CASE STUDY

Nonprofit Healthcare Organization Coordinates Better Care with BlackBerry

Industry:
Healthcare, Nonprofit

Region:
North America

Solution:
BlackBerry® Enterprise Service 10 (BES10), BlackBerry® 10, BBM®

Rocky Mountain Human Services (RMHS) provides resources, service coordination and training to nearly 10,000 individuals living with intellectual and developmental disabilities and veterans transitioning to civilian life. RMHS employs more than 400 professionals across Colorado and Wyoming, and offers several distinct programs ranging from mental health assessments, to brain injury support, to clinical and behavioral health therapies for children and families.

RMHS Rocky Mountain Human Services

The Challenge:

Based in Denver, Colorado, RMHS staff is spread out across the Rocky Mountains. They provide a range of services and supports including counseling for soldiers suffering from post-traumatic stress disorder, and clinical therapy groups for women with developmental disabilities.

"Part of my job as the IT Manager at RMHS is to ensure we have the right mobile infrastructure strategy in place," explained Frank Baer, IT Manager at RMHS. "Many of our employees, such as our Case Managers, are rarely at a desk and rely heavily on having information at their fingertips when meeting with a client. With this in mind, functionality was an important factor when considering mobile technology options. Security was also a top priority as our organization handles very private and sensitive client information."

"We provide our home-care staff with laptops, tablets and smartphones so they can update client information and communicate amongst their teams," said Baer. "Not only do we need to be able to manage those devices seamlessly, we need to be able to do it in an environment that adheres to the Health Insurance Portability and Accountability Act (HIPAA)."

RMHS needed to upgrade its enterprise mobility management (EMM) solution and smartphones to cost-effectively manage all of the devices on its network while keeping in mind HIPAA's stringent compliance and security requirements.

Key Benefits

- Improved employee communications
- Enhanced security
- Productivity-enhancing apps
- Cost-efficient EMM solution

> Our employees often require access to confidential information while in the field. The Citrix Receiver application allows for a seamless transition from employee workstations to our BlackBerry 10 smartphones, because we can access the same applications and files securely behind our corporate firewall.
>
> **Frank Baer, IT Manager at RMHS**

The Solution:

After years of partnering with BlackBerry, RMHS chose BlackBerry Enterprise Service 10 along with BlackBerry 10 smartphones to enhance its mobile productivity, meet the requirements of its employees, better serve its customers, and exceed its security needs.

“Before migrating to BES10, we were using BES5 and BlackBerry Curve and Bold smartphones. Integrating BES10 and the new BlackBerry 10 smartphones was easy for our IT department and also very intuitive for our employees,” explained Baer. “BES10 and BlackBerry 10 smartphones help us meet compliance and security requirements while maintaining a low total cost of ownership (TCO).”

RMHS’ Benefits:

Enhanced Productivity and Communication

Staff members who work at clients’ homes and administration professionals, including IT and finance, were transitioned to BlackBerry 10 smartphones. There was a minimal learning curve and seamless transition as users adapted quickly from their BlackBerry® Curve® and BlackBerry® Bold® smartphones to BlackBerry 10 devices.

“The nature of cognitive disabilities can make it difficult to have conversations with some clients and for them to relay their detailed medical concerns. With the BlackBerry 10 smartphones, we can quickly and easily use a smartphone to review case notes and access sensitive client records on demand,” said Baer.

Many RMHS employees spend the bulk of their time on the road. “It’s rare that I’m at my workstation or desktop. With my BlackBerry 10, I’ve created SMS email groups to more efficiently broadcast communications with my team and stay connected with both internal and external constituents,” explained Annie Davies, Director of Communications at RMHS. Auto synchronization to the server and universal access to it amongst staff has also made it easier to get in touch with colleagues.

BBM® is another useful tool that is being used to troubleshoot issues in the field. Case Managers can use BBM® Video conferencing to consult in real time with supervisors and collaborate remotely on the best course of treatment. During meetings, employees not physically present can share their screen and participate as if they were in the room.

Deploying BlackBerry devices with secure enterprise applications, such as Citrix Receiver or Documents To Go™, has tremendously reshaped how RMHS field workers do their jobs. Through these and other applications, RMHS employees can quickly pull information and review case notes from their devices, which proves to be easier and more secure than carrying around hard copies or laptops. A mobile solution also enables RMHS to achieve a high level of immediacy and ease of productivity. Employees also like having BlackBerry® Hub, which brings together work and personal emails and messages into a single convenient location so they can let their loved ones know what time they’ll be home for dinner.

Stronger Security for Patient Privacy

HIPAA established national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.

“Under HIPAA, even a patient’s name is protected, so accessing patient records through the RMHS-issued BlackBerry devices is safer than carrying around hardcopy files, a laptop or accessing them through a Wi-Fi network,” noted Baer. “With our employees on the road so frequently and constantly changing locations, it’s reassuring to know from a HIPAA compliance perspective that we can remotely disable an employee’s device if it is lost or stolen to ensure private information isn’t compromised.”

Beyond its encryption technology, BES10 also offers enhancements to enterprise security and manageability, including new IT policy controls and settings policies, S/MIME enhancements, Secure Voice support, Enterprise authentication enhancements and a new IT command to reset the Secure Work Space password. Having all devices under its control and ownership helps RMHS better serve and protect its clients, and do it within a nonprofit’s budget.

TCO of Home Care Businesses

One of the biggest challenges for home care businesses is increasing the quality of service provided to patients in their care. In a VDC 2006 Enterprise Mobility Service Survey of 120 healthcare professionals, about 69 percent of respondents identified quality of care and service as their top priority, followed by improved clinical data accuracy and improved billing information.

There are several ways to calculate the business value that mobile technologies can deliver to a home care business. This calculator can help you compute these benefits using metrics that are common to all organizations in the business of delivering home care services to people.

In our example, we will show how a home care organization with 1,000 employees can save between $2.8 million and $7.6 million on a recurring basis annually by implementing or improving mobile technologies. We have assumed that at least 20 percent or 200 of the employees are nurses, 60 percent or 600 employees are personal support workers (PSWs), while coordinators and back office support staff account for half each of the remaining 200 employees.

Table 1 shows the potential recurring cost savings resulting from reduced turnover costs, improved scheduling and dispatching, and improved worker productivity. All of these are factors that impact any home care business.

Table 1

Recurring benefits	Conservative estimate	Most likely cost
Overall recurring benefits	$2,884,243	$7,605,991
Quantified benefits	**Conservative estimate**	**Most likely cost**
Reduced turnover cost	$409,296	$1,058,913
Internal hiring cost avoidance	$300,000	$625,000
Education and training costs	$19,872	$74,813
Service disruption costs	$89,424	$359,100
Improved scheduling and dispatching	$438,019	$2,190,030
Improved worker productivity	$2,036,928	$4,357,048

To be quantified	Typical % improvements
Increased quality of care/service	68.70%

To be quantified	Typical % improvements
Improved clinical data accuracy	55.50%
Improved billing information	43.80%

In this example, this particular home care organization can reduce turnover costs by between $409,296 and $1,058,913.

To calculate turnover costs you need to consider three separate factors: internal hiring cost avoidance; education and training costs; and service disruption costs. Our sample organization can reduce turnover costs by $300,000 to $625,000, education and training costs by $19,872 and $74,813 and service disruption costs by $89,424 and $359,100.

Let's consider how we calculated the hiring cost avoidance numbers:

Table 2

Internal Hiring Cost Avoidance Baseline	$2,000,000	$3,125,000
Impact through technology	**15%**	**20%**
Total number of staff	1,000	1,000
Average turnover per month	2%	3%
Total number of turnover/month	20	25
Total number of turnover/year	240	300
Average time to hire (weeks)	4	5
Average no. of hours/week	40	40
Total no. of hours to hire	160	200
Average fully loaded cost/year	$100,000	$100,000
Total no. of working hours/year	1920	1920
Average fully loaded cost/hour	$52.08	$52.08

To calculate the internal hiring cost avoidance we first must determine how much the organization spends each year on hiring employees. In our example, we assume that the organization's turnover rate is approximately 20 to 25 employees per month, or 240 to 300 employees each year. These numbers appear to be the standard turnover rate in the industry. However, your organization's actual turnover rate may be higher or lower, so use numbers that are accurate for your specific situation.

After we have determined this employee turnover number, next we factor in the hiring time for a new nurse or personal support worker (PSW). In this example, we estimate that it would take the organization between four and five 40-hour weeks or between 160 hours and 200 hours to hire a single person. Again, your organization's ability to hire new people may be faster or slower. Finally, we factor in the cost per hour that the organization spends on searching for, vetting, and hiring new staff. In our example, the fully loaded cost works out to $52.08 per hour.

If we do the math, it means that our sample organization conservatively spends roughly $8,332 to hire one employee or about $2 million annually to hire 240 new workers (52.08 X 160 X 240). Our "most likely" estimate using the same math is approximately $3,125,000 per year on hiring new employees (52.08 X 200 X 300). Our research shows that organizations can decrease this cost by 15 percent to 20 percent through the use of enterprise mobility technologies. That means the internal cost avoidance for our sample organization would be between $300,000 and $625,000.

We could apply a similar logic for computing the reduction in education and training costs, service disruption costs, and the impact on patient care. To compute education and training costs for instance, consider the amount of time you spend on training, the number of nurses and PSWs you need to train each year, and the average hourly wages for them:

Table 3

Education and Training Cost	$99,360	$299,250
Impact through technology	20%	25%
Average training time (hours)	40	50
Hourly wage for nurses	$20.00	$60.00
Hourly wage for personal support workers (PSWs)	$10.50	$10.60
Total number of turnover/year	240	300
% of nurse turnover	15%	20%
% of PSW turnover	70%	75%
Total cost of Nurse education	$28,800	$180,000
Total cost of PSW education	$70,560	$119,250

This example assumes that the organization spends 40 to 50 hours training a nurse, costing $20 to $60 an hour. That works out to $800 to $3,000 in training costs per nurse, or $28,800 to $180,00 annually to train between 36 and 60 nurses, if we were to assume a turnover rate of 15 to 20 percent. We use the same math to compute the total cost of educating and training PSWs, for an estimated training cost of $99,360 to $299,250 annually.

At a 20 percent impact using enterprise mobility technology, the organization would save between $19,872 and $74,813 on education and training.

Plug in your own numbers above to estimate the business value that mobility can bring to your home care organization.

Chapter 8

mHealth

Mobile Health – the Transformative Frontier

By Pramod Gaur, PhD, Chair mHealth SIG, American Medical Association and Adjunct Professor, Pace University

Mobile healthcare, or mHealth, has become another buzzword in an industry already filled with them. It can be confusing, though, to understand what different mobile technology vendors mean when they talk about mHealth. For the sake of this discussion, we will focus on mobile and embedded devices designed for use in hospitals and other healthcare environments rather than wearable consumer products such as fitness monitors.

According to the *National Institute of Health's* Office of Behavioral and Social Science Research, "mHealth has the potential to change when, where, and how healthcare is provided; to ensure that important social, behavioral, and environmental data are used to understand the determinants of health; and to improve health outcomes."

"40 percent of patients would pay a monthly fee for remote monitoring devices that would send data to their doctors automatically, according to research from the consulting firm *PricewaterhouseCoopers' (PwC) Health Research Institute (HRI)*. It's evidence that mHealth is not a service that must be sold to patients, but rather an opportunity to provide excellent healthcare and meet a growing demand. As PwC put it: "Remote monitoring could be a key way to reduce office visits. Eighty-eight percent of physicians said they would like their patients to be able to track and/or monitor their health from home... remote monitoring could be especially effective at reducing hospital readmissions. Research has shown that one-fourth of all Medicare patients are readmitted within 30 days."

> "While mHealth is just one part of a healthcare facility's outreach to the public, it is an important component to both providing care and improving patients' wellness."

> For physicians and other medical personnel, mobile mHealth solutions are some of the most effective ways to remotely monitor patients.

Having information at their fingertips also assures physicians that their time is used more effectively, says PwC. Of physicians who are using mobile devices in their practices, 56 percent say the devices expedite their decision-making and nearly 40 percent say they decrease administrative time. These are impressive results.

The robotic doctors that many of us remember from the 1960s-era cartoon The Jetsons is closer to reality today than many of us realize. However, The Jetsons didn't get it 100 percent right: in reality, that "robotic doctor" might simply be a Bluetooth® enabled embedded device feeding vital signs to the physician or an implanted heart valve that feeds back data to let doctors know how well the patient's heart is working. Similarly, the 1960s vision of shrinking a submarine full of surgeons in order to enter a person's body in order to operate, as in the Fantastic Voyage, is coming to fruition in the form of miniaturized camera-controlled surgical tools (though shrinking humans remains beyond our technology for now).

Mobile health is transformative indeed. Among the changes we are seeing in mHealth is not only a difference in the types of devices used by healthcare providers, but also a sea change in the way that healthcare is provided.

mHealth is making its most significant strides in two specific areas: home healthcare and emerging geographical markets. Let's focus on home healthcare. Medical professionals are always looking for an edge when it comes to identifying potential health problems. However, in-facility tests are often either inappropriate or inconvenient. Take for example the diagnostic testing for cardiac arrhythmia. Today's testing methods are cumbersome and can take several weeks from the doctor's original visit to diagnosis.

At *m-Health Solutions*, the firm developed a technique that uses mobile technology to speed up and improve the diagnosis of cardia arrhythmia. mHS uses a BlackBerry smartphone, a custom application and a hybrid cardiac diagnostic device to record cardiac activity for up to two weeks. The recorder transmits data via Bluetooth to the phone, which in turn transmits the data to a diagnostic center where the data is analyzed by a cardiac technologist. The tests provide superior clinical information about the patient's heart activity, reduce wait time for diagnostic tests, enable an earlier diagnosis of cardiac conditions, and are more convenient for both patients and doctors.

Medical professionals, in-home providers and first responders can have the appropriate patient's medical records at hand when necessary. Efficient, high-quality medical care becomes easier to deliver as embedded devices and sensors, along with smart phones or tables, create powerful diagnostic and analytic tools at the patient's or client's home.

While mHealth is just one part of a healthcare facility's outreach to the public, it is an important component to both providing care and improving patients' wellness. It spans a variety of capabilities central to the concept of healthcare rather than sick care. By providing resources to patients that help them stay well and manage their wellness, mHealth becomes an important part of their personal health program.

For physicians and other medical personnel, mobile mHealth solutions are some of the most effective ways to remotely monitor patients. It's one of the most exciting trends in the healthcare industry and is expected to grow exponentially in years to come.

Pramod Gaur, PhD, is a visionary leader with extensive record of achievement in commercializing telehealthcare, medical devices and diagnostics technologies. His activities as a telehealth industry advocate include demonstrations to the US Presidential Advisor, US Congress on Capitol Hill, The White House Conference on Aging and to International Delegates at the United Nations. Dr. Gaur has volunteered his time to the American Telemedicine Association (ATA) in various roles, including as Chairman of ATA Industry Council, one-year term on ATA Board of Directors and two-year term as Chair of ATA International SIG. He is currently serving as Chair of ATA mHealth SIG. Dr. Gaur was inducted in ATA College of Fellows in Class of 2013.

CASE STUDY

First Responders in India Rely on BlackBerry and eUno to Attend to Cardiac Patients in Near Real Time

Industry:
Healthcare

Region:
Asia Pacific

Company Size:
Large Organization

Solution:
BlackBerry® 10 smartphones, BES, eUNO solution by Maestros

maestros
enabling technology for you

Central Railway Hospitals is an organization operated by the Indian Government and a subsidiary of the Ministry of Railways. Central Railway Hospitals serves a large part of the Indian population by providing comprehensive healthcare services to current and retired Railway employees and their dependents. Central Railways provides an emergency cardiac-care facility onboard for passengers travelling on trains at various stations. This facility is also available to passengers on platforms waiting to board the trains.

The Challenge:

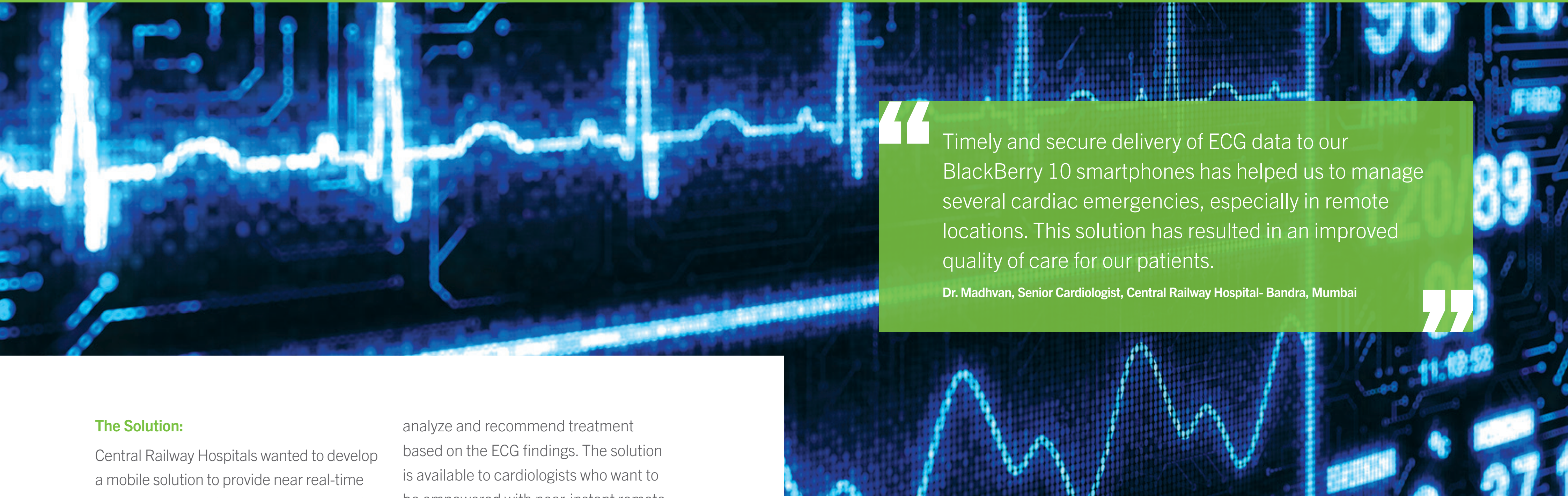
According to Indian government data, heart failure incidences in India range up to 1.8 million annually. To manage the health of heart patients, it is advisable to monitor his or her condition through regular ECG reports and consult a professional in a timely manner. Despite a huge number of hospitals and a wide network of medical facilities, it is challenging to provide patients who are riding on the Indian Railways network the care they need when they experience a cardiac event.

Central Railway Hospitals provides medical services on moving trains and stations in remote locations all across India. The cardiac team at Central Railway Hospitals were looking for a way to quickly address cardiac emergencies. The issue of cardiac emergencies poses a serious threat to a country as populated as India, especially in rural areas where care is not immediately accessible. In such cases, it becomes critical to quickly get the necessary medical help.

“Time is of the essence when you’re talking about a patient in need of care during a cardiac emergency,” said Dr. Sushma Mate, Tele-Cardiology Solution Support Team, Central Railway Hospitals, Byculla-Mumbai. “You have a short window of time to get the patient’s ECG information to a cardiologist, diagnose the problem, and get the patient the treatment they need. We knew that mobile connectivity for data transfer could make our processes faster and our treatment times shorter.”

Key Benefits

- Improved response time for patients having a cardiac emergency
- Highly secure transmission of patient data
- Improved quality of patient care in remote locations



> Timely and secure delivery of ECG data to our BlackBerry 10 smartphones has helped us to manage several cardiac emergencies, especially in remote locations. This solution has resulted in an improved quality of care for our patients.
>
> **Dr. Madhvan, Senior Cardiologist, Central Railway Hospital- Bandra, Mumbai**

The Solution:

Central Railway Hospitals wanted to develop a mobile solution to provide near real-time updates in cases of cardiac emergencies for passengers riding the rail lines. A long-time BlackBerry customer, they partnered with Maestros Mediline Systems Limited, a leader in the design of diagnostic and patient monitoring devices, to create a mobile application that securely connects to cardiac monitoring hardware and transmits ECG data to cardiologists using BlackBerry 10 smartphones.

The eUNO solution records heart activity and, when connected to the Internet, sends a 12-lead ECG to the medical records server. Using BES, the ECG report is automatically routed to a doctor's BlackBerry 10 smartphone so they can analyze and recommend treatment based on the ECG findings. The solution is available to cardiologists who want to be empowered with near-instant remote access to patients' ECG and heart performance reports while on the go, allowing them to respond quickly with a diagnosis and prescribe appropriate treatment. The solution works over both Wi-Fi® and cellular networks.

"Because of the security of the BlackBerry platform, we are able to safely and quickly deliver critical patient ECG data to doctors and clinicians," said Sunil Buva, Business Head, Tele-Health products, Maestros. "This allows us to meet the needs of the emergency cardiac-care segment effectively while also being mindful of security around patient data."

Central Railway Hospitals Benefits:

Security and privacy are of utmost importance in the healthcare industry. "We have confidence that the BlackBerry smartphones managed by BES are secure," Dr. Mate explained. "We can enforce policies, such as password protection, and if a device is ever lost we can remotely wipe it, so we have full control and management of the devices."

Since deploying the eUNO solution on BlackBerry 10 smartphones, Central Railway Hospitals have witnessed a remarkable increase in response time. Doctors are able to receive ECG data on their BlackBerry smartphones within five minutes. This has enabled early detection of heart attack cases, allowing for faster treatment and medical guidance. To date, nearly 5,000 ECG reports have been transmitted by Central Railway Hospitals using the eUNO solution and it has enabled the team to identify true cardiac emegerncies and treat them accordingly.

"Timely and secure delivery of ECG data to our BlackBerry 10 devices has helped us to manage several cardiac emergencies, especially in remote locations," said Dr. Madhvan, Senior Cardiologist, Central Railway Hospitals- Bandra, Mumbai. "This solution has resulted in an improved quality of care for our patients."

CASE STUDY

BlackBerry Solution Used to Monitor Patients Helps Provide Faster and More Convenient Way to Detect Cardiac Arrhythmia

Industry:
Healthcare

Region:
North America

Company Size:
Small

Solution:
BlackBerry® smartphones, BlackBerry® Enterprise Server (BES), m-CARDS™ (Mobile Cardiac Arrhythmia Diagnostic Service), a custom application developed in-house

m-Health Solutions is a Canadian company, based in Burlington, Ontario, working in the growing field of mHealth technology, a term describing the use of mobile devices for the collection and distribution of health data, remote delivery of care and near real-time monitoring of patients. m-Health Solutions provides doctors and patients with a fast and convenient diagnosis system to help detect cardiac arrhythmia and asymptomatic atrial fibrillation. Both the technology and the service are covered under the government's health insurance plan.

The Challenge:

Medical professionals are always looking for ways to detect heart conditions and preventatively treat heart disease and stroke. Many lifesaving technologies and treatments are available, however before these can be used, a patient requires a diagnosis. One of the major challenges facing physicians is being able to quickly access technologies that will help them monitor and diagnose patients at risk.

To make a diagnosis, family physicians often refer patients to cardiologists. One of the most familiar tests currently available is a device called a Holter monitor that records cardiac activity for 24 to 48 hours. The device typically requires 5 to 7 leads, cannot be removed to bathe, and the patient must make several trips to a hospital and clinic to be started on the device, to return the device and then to receive the results.

Key Benefits

- Earlier diagnosis of cardiac conditions
- Better clinical information about a patient's heart activity
- Reduced wait time for diagnostic tests
- Greater convenience for patients and doctors

"The Holter monitor test is cumbersome and can take several weeks to deliver results," said Sandy Schwenger, Co-owner and CEO of m-Health Solutions. "We knew earlier diagnosis and treatment could mean better patient outcomes and the best way to get to a patient early was through the first doctor the patient sees when complaining of symptom. Often this is the family doctor. As well, it was critical that the patient has access to a technology that provided faster diagnosis."

> “With the help of BlackBerry smartphones and our mHealth technology, family doctors and specialists can make a faster diagnosis of a person at risk, meaning the patient can access the latest technologies and medications leading to potentially better outcomes.”
>
> **Sandy Schwenger, Co-Owner and CEO, m-Health Solutions**

The Solution:

To speed up the process of diagnosing or ruling out cardiac arrhythmias, m-Health Solutions developed the Mobile Cardiac Arrhythmia Diagnostic Service m-CARDS™, a solution for family doctors, internists, neurologists and cardiologists. When a patient reports suspicious symptoms, the doctor can initiate the test right away, without sending the patient to the hospital or a specialist.

During the initial visit, the doctor attaches two electrodes to the patient, explains what the test is for and what to expect. They then send a requisition form to m-Health Solutions. Within 24 to 48 hours, a kit arrives at the patient's house or office containing a hybrid cardiac diagnostic device – which continuously monitors cardiac activity for up to two weeks – a BlackBerry smartphone and user instructions.

To learn how to hook-up the device, patients can either view video instructions on the BlackBerry smartphone, DVD or m-Health Solutions web site or read the written instructions provided in the kit. Once attached, the device starts to transmit data via Bluetooth® to the BlackBerry smartphone. The BlackBerry smartphone sends the information to m-Health Solutions at its diagnostic centre where it's interpreted by cardiac technologists. The company also uses the BES to manage, control and push software updates out to the devices.

“We did research that told us people are ready and able to embrace mHealth solutions,” said Schwenger. “We've found that people of all ages are able to hook it up without much trouble – even people in their 80s who have never operated a computer.”

Patients are monitored in ‘near real time’ and as soon as there are results, m-Health Solutions cardiac technologists post the report for the cardiologists. They then use a secure portal to make a diagnosis from virtually anywhere in the world. At any point during the test, a technologist can flag an abnormality. Patients can also report the onset of a symptom by pressing a button on the recorder and entering details using a drop-down menu on the BlackBerry smartphone.

The cardiologists are able to electronically sign off on the results, which are then faxed to the referring doctor within approximately 24 hours of the patient completing the test for follow-up care.

m-Health Solutions' Benefits:

m-CARDS allows family physicians, cardiologists, neurologists, and other specialists to order an easy-to-use, 'at-home' diagnostic test as soon as the patient presents symptoms. The BlackBerry smartphone transmits data in near-real-time, which helps avoid the delays associated with downloading the results at the completion of the test. The interpreting cardiologist can then review the findings, and report them almost immediately which helps to speed up treatment time.

"The investigation and diagnosis of cardiac issues was often a drawn out process," said Schwenger. "After seeing your family doctor, it could take days or weeks to see a specialist and several more weeks for diagnosis. With m-CARDS, the patient is typically hooked up within 24 - 48 hours of seeing the referring physician, neurologist or other specialist meaning patients may be treated sooner."

Schwenger believes that m-Health Solutions is an effective way to help identify an event quicker than ever before. "Before m-CARDS, patients only had access to technologies that may not be easy to use; were inconvenient, could produce poor diagnostic results and took far too long in getting results back to referring physicians," said Schwenger. "Then they would have to wait and worry about whether something was seriously wrong. Now, with the help of BlackBerry smartphones and our mHealth technology, family doctors and specialists can make a faster diagnosis of a person at risk, meaning the patient can access the latest technologies and medications leading to potentially better outcomes."

For stroke patients, being able to be monitored as soon as possible is especially important as the m-CARDS solution can detect rhythms that may trigger a secondary stroke. 25 percent of strokes and 50 percent of TIAs (Transient Ischemic Attack, or mini-strokes) are of "cryptogenic" or unknown causes. m-CARDS has the ability to identify these asymptomatic rhythms which could have caused the first stroke allowing patients to get on medication sooner and potentially prevent further incident.

"The hybrid cardiac diagnostic device, in combination with the BlackBerry smartphone, helps provide a greater diagnostic yield than traditional two-day monitors," said Schwenger. This solution has been well-received among doctors and patients. Currently, 1800 family physicians throughout Ontario have chosen to access m-CARDS to arrive at a diagnosis for nearly 23,000 patients.

"With BES, we are confident that our data is safe and secure. It also allows us to push out software updates and disable a lost or stolen device remotely which provides us with great peace of mind," said Schwenger. "We believe this BlackBerry solution is just the beginning in helping to improve the diagnosis, treatment and management of cardiac diseases and disorders. We are already in the process of looking to expand this solution to other provinces in Canada."

The Impact of Mobile Healthcare on Patient-Provider Consultations

By Lisette Lockyer, Pediatric Nurse Practitioner, Alberta Children's Hospital

Healthcare isn't solely about awe-inspiring breakthroughs in detecting and treating illnesses. At the core of medical care is the dialogue that occurs between patients and health professionals. These interactions can have profoundly positive impacts on patients' prognoses, according to a 2014 review of 13 clinical trials published in the journal *PLOS One*. These results and other similar studies help validate traditional aspects of healthcare practice, such as in-depth interactions, ongoing relationships between patients and healthcare providers, and even house calls.

Looking forward, the integral part patient-provider communications play in patients' well-being highlights the potential of mobile patient-provider communication solutions. These solutions promise increased flexibility and greater efficiencies as patient-provider consultations evolve from in-person appointments to video consultations and two-way messaging. Another element to consider is the newly legislated Stage 2 Meaningful Use criteria, which mandates an increasing health information exchange between patients and healthcare providers. As providers continue to look to meet the Meaningful Use requirements, finding new ways to securely communicate with patients will become more important than ever.

> "The number of home monitoring systems with integrated cellular connectivity is expected to be a little more than seven million worldwide by 2017."
>
> *Source: Berg Insight*

But while the importance and benefits of mobile patient-provider communication solutions are clear, to date their widespread adoption has been labored. For example, the number of home monitoring systems with integrated cellular connectivity is expected to be a little more than seven million worldwide by 2017, according to a report issued by *Berg Insight* on mobile health and home monitoring. Widespread adoption of telemedicine solutions has been stunted for reasons ranging from data protection concerns and cost to cumbersome equipment and an unreliable experience.

A holistic reimagining of patient-provider communications is key to resolving these problems. It's a strategy with three key parts: 1) mobile devices that are cost-effective but allow for visually rich experiences; 2) specifically designed applications that enable secure real-time sharing of health data; and 3) a cross-platform EMM solution which provides a secure communication infrastructure. These elements allow for an experience that includes the hallmarks of an in-person consultation, but frees healthcare professionals and patients to talk to each other wherever they are.

Mobile health solutions tackle the inefficiencies and costs associated with in-person consultations. Consider this example. A patient is seen in the emergency room, is treated and sent home. The treating physician often follows up with the patient via telephone but often ends up leaving a voicemail. The patient calls back to find the doctor unable to take the call. And the phone tag continues.

Consultations conducted using a mobile health platform reduce costs and are a more convenient option for both the medical provider and their patients. A mobile solution that allows patients and providers to communicate using secure messaging means neither party needs to be on hand. The communication can be escalated to a voice call, video conference and even screen sharing. A post-operative patient recovering at home or a patient who lives a great distance from a healthcare facility are just other of the many scenarios where patients benefit from mobilizing patient-provider communication. In fact, more than 200 million people in the United States and Europe suffer from diseases in which mobile-based consultations could be an option, according to the Berg Insight report.

Patients are willing to embrace telemedicine as long as it delivers an improved experience. Fifty-two percent of respondents to a *2011 Forrester survey* about the adoption of mobile healthcare were willing to use a health-related assessment app if it provided faster access to care.

But with new technology often comes new risks. The public currently has a relatively high sense of confidence in the safety of their medical records. In the Forrester report about mobile healthcare, 78 percent of respondents indicated that their privacy and confidentiality are well protected. But public sentiment, can swing dramatically. It's unlikely the public's confidence could withstand a highly-publicized security breach like that experienced at Target, Inc. and other major retailers in recent years. According to a study conducted by the *Ponemon Institute*, more than 90 percent of healthcare organizations reviewed had had a data breach.

In the context of mobile communications, there is likely to be increased scrutiny, and as a result less tolerance, from patients and government regulators for data breaches. This makes it even more important that mobile patient-provider communication solutions include a security infrastructure that is both well developed and seamlessly integrated so that both medical professionals and patients can be assured that their communications are as private and confidential as if they were in the same room.

Mobilizing patient-provider communication solutions allows consultations between healthcare professionals and patients to enter a new era in which physical location isn't a barrier. An expanded population around the world, namely those in rural and remote locations, will gain the level of access to medical care that's currently only available to those in more urban settings. Patients can be monitored for post-operative care once they leave the hospital, and connect back to their specialist if they have any issues or questions, resulting in better patient outcomes because this relationship is maintained. Healthcare providers can conduct consultations using video, phone, or messaging in a secure way, confident that the privacy of patient data is maintained. Providers can also communicate with patients as they make the transition from hospital to home.

> “Surveys show patients are willing to embrace telemedicine as long as it delivers an improved experience or faster access to care.”

With secure mobile solutions for patient-provider communication, patients will once again be receiving house calls.

Lisette Lockyer is a pediatric nurse practitioner at Alberta Children's Hospital.

Top Indian Hospital Leverages BBM Video and Remote Health App on BlackBerry for Patient Monitoring

Industry:
Healthcare

Region:
APAC

Company Size:
Large Organization

Solution:
BlackBerry® 10 smartphones, BES, BBM® Video, UST Global Mobile Telemedicine app

Dr. L H Hiranandani Hospital (Hiranandani Hospital), ranked among the top 10 quality hospitals in India and Asia, is one of the few multi-specialty hospitals in the country and the only one in Mumbai and western India to have received accreditation by the National Accreditation Board for Hospitals and Healthcare Providers (NABH) and accredited through ISO 9001: 2000 certification. Recognized as having high levels of infrastructural strength and technical competence, Dr. L H Hiranandani Hospital offers superior high-end critical care services.

The Challenge:

There is a dire need to bridge the massive urban-rural gap that exists in India. A sizeable chunk of India's rural population is deprived of basic healthcare facilities. Less than 25 percent of India's specialist physicians reside in semi-urban areas and a mere three percent live in rural areas. As a result, rural areas with populations approaching 700 million continue to be limited in their ability to access medical specialists.

As many patients in rural India have limited access to basic healthcare services, healthcare teams in these remote locations needed an easier way to treat more patients, and consult with medical specialists that would not otherwise be available. In the past, remote healthcare teams had to rely on landlines and desktop computers equipped with video capabilities, which added costly IT infrastructure and hindered mobility. On the physician's side, they needed to be able conduct consultations easily from wherever they were, as opposed to having to travel to remote locations, or specialized telemedicine centers, in order to treat patients.

Key Benefits

- Secure infrastructure for remote teleconsultations, diagnosis and opinion sharing between healthcare professionals and their patients
- Improved access to medical specialists in rural areas
- Improved patient outcomes
- Reduced IT infrastructure costs of 80 percent

BlackBerry and UST Global won a 2015 *Aecus Innovation award* for this mobile telemedicine app that enables remote patient healthcare.

"We needed to find a solution to address a unique challenge in our healthcare system," said Dr. Pavan Kumar, Consultant Cardiac Surgeon, Head - Telemedicine Center, Hiranandani Hospital. "We had to find a way to enable our medical professionals to remotely monitor patients' health and provide quality care from a distance."

The Solution:

Under the guidance of Hiranandani Hospital and in partnership with BlackBerry India, UST Global developed a mobile telemedicine app which provides access to qualified doctors and affordable treatment without the need for patients to travel to cities, and without requiring physicians to be at a special telemedicine center. The first deployment is for a telemedicine network which provides services to over 100 peripheral hospitals in India and Africa.

The telemedicine app on BlackBerry 10 devices allows patients, doctors, specialists and peripheral hospitals to conduct teleconsultations, provide diagnoses and collaborate on patient care, all through the security of the BlackBerry platform. It uses BBM® Video to enable video sessions between the clinical staff, the patient and the specialist.

"BBM® Video has been a great tool for us to communicate with patients in rural areas," said Dr. Pavan. "Cellular connectivity is often more reliable than landlines in some areas, so BBM® Video is an excellent solution to meet our needs. The ability to connect and see our patients in real-time is incredibly powerful."

The telemedicine solution is secured through BES which ensures sensitive patient data is kept private and also provides secure connectivity to backend databases and systems. Building on the BlackBerry platform has allowed for multi-OS device support to mobilize the solution on other devices as well. BES provides robust application management and push services for real-time updates and notifications on the device which has resulted in improved workflow.

"UST Global believes in placing consumer-centricity and innovation at the heart of our solutions to transform lives in the communities that we operate in," said Gilroy Mathew, General Manager of UST Global. "The mobile telemedicine application helps to eliminate distance barriers and to improve access to medical specialists that would often not be consistently available in distant rural communities. We built this solution on BlackBerry to ensure the security and privacy of patient data, as well as to allow interoperability with other mobile platforms."

Hiranandani Hospital's Benefits:

The deployment of the mobile telemedicine app has expanded the reach of Hiranandani Hospital by enabling its healthcare teams to access more patients without having to physically travel to other locations. Rural communities are now able to meet the unique challenges of maintaining access to healthcare at an affordable price. With the telemedicine app, it is less cost prohibitive for remote patients to obtain timely medical care for common and treatable ailments, since they don't need to pay for travel to a large city. And, Hiranandani has already seen an 80 percent reduction in IT infrastructure costs using the BlackBerry solution compared to using their previous solution of landlines and desktops.

> "The BlackBerry platform is a perfect match for this ground breaking app in healthcare as it provides BES for world-class security, hardware to match our requirements, and integrates BBM Video for videoconferencing. The Telemedicine app allows teleconsultations, diagnosis and opinion sharing between patients, doctors, specialists and peripheral hospitals, all through the security of the BlackBerry infrastructure."
>
> **Dr. Pavan Kumar,**
> **Consultant Cardiac Surgeon, Head – Telemedicine Center, Hiranandani Hospital**

Patients can be monitored for post-operative care once they leave the hospital, and connect back to their specialist if they have any issues or questions. This results in better patient outcomes because the doctor-patient relationship is maintained and the condition can continue to be monitored by the same specialist that administered the original treatment. For the IT department at the hospital, the solution has eliminated the need to purchase expensive equipment and costly infrastructure to support the rural communities.

"We wanted to simplify and build a comprehensive telemedicine app which would achieve the main functions of a desktop system, but on a smartphone," said Dr. Pavan. "The BlackBerry platform is a perfect match for this ground-breaking app in healthcare as it provides BES for world-class security, hardware to match our requirements, and integrates BBM Video for videoconferencing. The telemedicine app allows teleconsultations, diagnosis and opinion sharing between patients, doctors, specialists and peripheral hospitals, all through the security of the BlackBerry infrastructure."

Chapter 9

Connecting and Securing the Healthcare Internet of Things (IoT)

BlackBerry's Technologies: Securely Connecting and Managing Healthcare Things

By Sandeep Chennakeshu, President, BlackBerry Technology Solutions

Healthcare has become mobile to a degree undreamed of a generation ago. Today doctors can access everything from patient records to the latest genome research on a smartphone. EMTs can send high-resolution photos of a patient's injuries from their smartphones to the ER in seconds. Nurses can save time by sending secure texts to doctors and other healthcare staff, using BlackBerry's BBM® Protected messaging. Using BES®12, the BlackBerry cross-platform Enterprise Mobility Management (EMM) solution, hospitals can securely manage a fleet of smartphones and tablets for all of these medical communications whether the devices are BlackBerry or employee-owned iOS®, Android™, and Windows Phone® devices.

Now healthcare is entering a new phase of Internet connectivity that goes beyond smartphones. Think of the confluence of Internet of Things (IoT) and healthcare. Healthcare IoT envisions every healthcare device equipped with an Internet connection so that it can communicate securely with other devices to report its status and the status of the patient that the device is monitoring. Pacemakers, blood glucose monitors and other familiar devices have already become healthcare IoT-enabled for faster data collection and analysis.

> "Pacemakers, blood glucose monitors and other familiar devices have already become healthcare IoT-enabled for faster data collection and analysis."

As more medical devices come online in hospitals and homes, their speed and convenience promise enormous cost and health benefits. Doctors, nurses, and patients will have the precise care information they need exactly when they need it. No more manual checks of equipment such as defibrillators or infusion pumps to ensure they are working properly. No more unnecessary trips to the doctor's office for the sick and elderly. No more tracking devices in hospitals, where loss and time spent locating devices costs thousands of dollars per bed.

The challenge of healthcare IoT is to manage all of this data remotely and securely with best-in-class security, privacy and intelligent data management – from a central console. This is where BlackBerry's secure mobility expertise, QNX® Neutrino® real-time OS, Certicom's elliptic curve cryptography (ECC) and BlackBerry's IoT platform come in.

QNX Will Run It

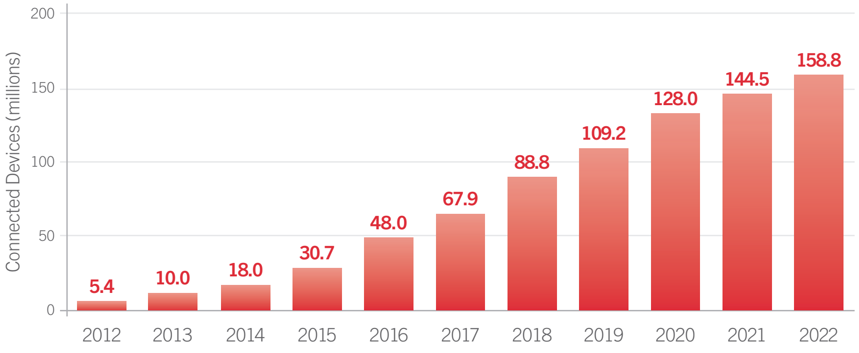
Over the last 35 years, QNX embedded software has quietly revolutionized how we live. People encounter QNX-controlled systems whenever they drive a car, watch TV, use the Internet, undergo laser surgery or even turn on a light. Its ultra-reliable nature means that QNX is the preferred choice for mission-critical systems such as train control systems and nuclear power plants. Because the QNX CAR™ Platform and QNX Neutrino OS also support rich multimedia frameworks and user interfaces, they are used in the latest in-dash automotive infotainment systems and digital instrument clusters. More than 40 carmakers in all, including Ford, Audi, GM, and Volkswagen, use QNX in their latest models to provide fast, reliable, and smooth-operating entertainment, GPS, and other in-car information systems.

With its purchase of QNX Software Systems Limited in 2010, BlackBerry became the leader in automotive telematics and infotainment software, the foundation to be a leader in Internet-connected cars.

QNX software has been deployed in more than 60 million automobiles and, according to the research firm IHS Automotive, is the clear leader in car infotainment software, with more than 50 percent market share. In addition, QNX acoustic solutions such as active noise cancellation and echo suppression have shipped in 40 million cars to date, with about a million new cars enabled every month.

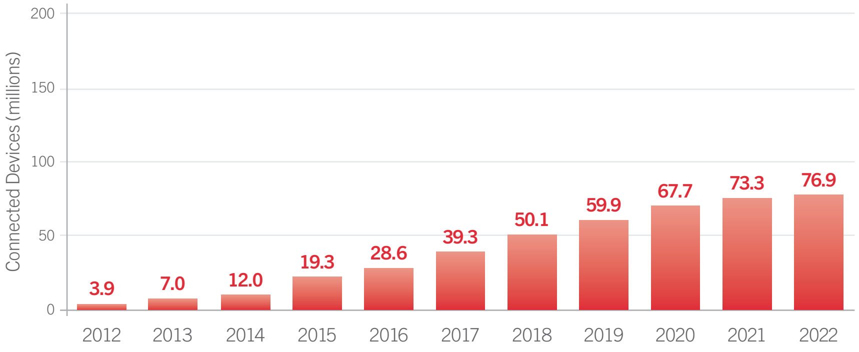
QNX boasts an equally impressive resume of deployment in medical equipment ranging from blood analyzers, retinal scanning devices, and vital signs monitoring equipment to pulse oximeters and eye surgery lasers. QNX software controls surgical machines that precisely mill bone surfaces in orthopedic procedures, and other surgical systems that let doctors perform delicate operations using robotic arms. QNX Neutrino is a real-time OS that offers IEC 62304 Class C compliance for medical device software, along with integrated remote management capabilities for secure configurations, updates, monitoring, data transmission and storage.

Assisted Living – World



Source: Machina Research

Clinical Remote Monitoring – North America



Source: Machina Research

Certicom Will Protect It

Certicom® is another BlackBerry wholly owned subsidiary that specializes in elliptic curve cryptography (ECC) solutions. The advantage of ECC over traditional RSA® cryptography is that one can use significantly shorter encryption keys for the same level of security. ECC is inherently more efficient for resource-constrained medical devices, which are battery-operated with small processors and memory. Certicom's technology can be used to authenticate devices, authorize them to connect to the enterprise, and encrypt messages for privacy.

> When every critical piece of the healthcare puzzle can be monitored for improvement, healthcare professionals will be better equipped than ever to provide excellent care.

BlackBerry IoT Connects it All

Last year, BlackBerry introduced its BlackBerry® IoT Platform, which leverages BlackBerry assets including its global secure network, QNX embedded software, Certicom ECC, low-power device connectivity and BES12. The aim of the BlackBerry IoT platform is to connect IoT devices wirelessly and transfer their data in a secure manner to only those people or enterprises who have the permission to view the data. Global coverage, scalability, end-to-end security, privacy and fine-grained permissions are hallmarks of BlackBerry's IoT solution. Further, tens of thousands of companies use BES12 to easily and securely manage their smartphones. On the BlackBerry IoT Platform, BES12 will expand in management capabilities to oversee a variety of other devices, including healthcare hardware. BlackBerry's IoT platform allows lifecycle management of devices by being able to diagnose faults and updating software over the air (OTA) throughout the device's lifetime. BlackBerry's OTA software is proven in updating tens of millions of mobile phones in over 100 countries globally.

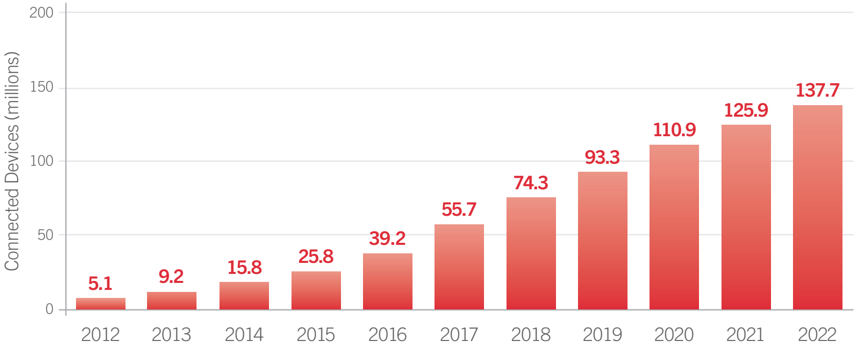
In The Real World

BlackBerry is designing a unique solution to track and trace pharmaceutical drugs as they ship from the manufacturer to the hospital. The solution is based on Certicom's patented compact digital signatures to sign drug labels and track these as they pass through the supply chain using the BlackBerry IoT platform and managed public-key encryption system. This solution can prevent theft and counterfeiting, promoting a safer and more reliable supply chain for pharmaceutical drugs.

A Win For Patients

As we take this next step in connectivity with IoT, the possibilities for better healthcare are endless. However, transformative changes also bring new potential risks in security and privacy leaks. BlackBerry delivers proven security expertise and software solutions to let healthcare organizations tap into IoT while protecting patient data – and lives. When every critical piece of the healthcare puzzle can be monitored for improvement, healthcare professionals will be better equipped than ever to provide excellent care. Patients win, caregivers win and the healthcare system wins.

Clinical Remote Monitoring – World



Source: Machina Research

Dr. Sandeep Chennakeshu is the President of BlackBerry Technology Solutions (BTS). In this role, he manages and drives the strategic direction of BlackBerry's innovative technology assets, including QNX Software Systems (embedded software), Certicom (cryptography applications) and Paratek (RF antenna tuning). Sandeep also manages the company's extensive patent portfolio and Internet of Things business.

How BlackBerry Is Securing the Healthcare Internet of Things

By David Kleidermacher, Chief Security Officer, BlackBerry

The Internet of Things (IoT) is here and brings a wealth of new benefits for healthcare organizations. As more medical devices become capable of connecting to the Internet, hospitals have a chance to monitor patients more closely and efficiently. Closer attention brings better patient care, and that can translate into savings in time, money, and patients' lives.

With IoT, healthcare providers will need to focus on security more than ever. Modern hospitals operate complex networks connecting caregivers, equipment, and patients. The traditional wired network and the wireless smartphones and tablets that it supports will be joined by a growing number of connected medical devices. Although IoT offers huge opportunities, it adds to the pressures hospitals already face in protecting their networks. The attack surface available to hackers naturally grows over time, and IoT has the potential to exponentially increase attack vectors by adding millions of new devices to large organizations. Hackers are adept at exploiting weaknesses, whether in an unpatched operating system, a downloaded app, or simply human error. Once inside the healthcare provider's internal network, the attackers can directly attack the organization's Internet-connected devices. So how can healthcare providers protect their networks against these attacks?

> Although IoT offers huge opportunities, it adds to the pressures hospitals already face in protecting their networks.

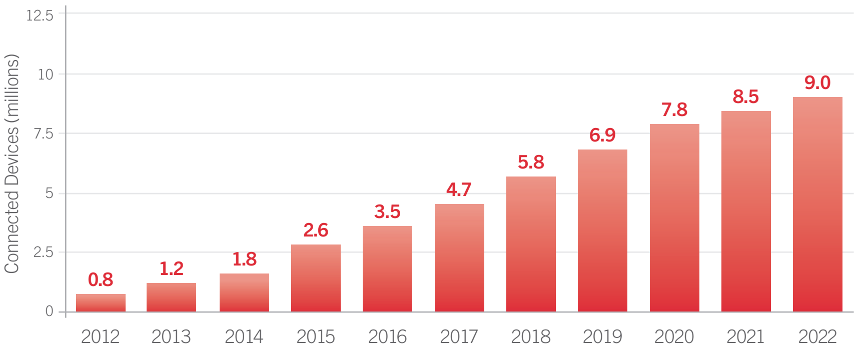
BlackBerry Pushes the Envelope

BlackBerry is already helping healthcare organizations secure themselves for IoT. Organizations such as Mackenzie Health are using our platform to securely manage and route data from smart, connected medical devices, such as sensor-enabled 'smart beds', staff ID badges and handwashing stations that track how often doctors and nurses clean their hands.

Earlier this year we announced a new security initiative called the Center for High Assurance Computing Excellence (CHACE). The BlackBerry CHACE team has been busy establishing cooperative research relationships with universities, including the University of Oxford in the United Kingdom, Cal Poly San Luis Obispo and University of California in Santa Barbara in the United States, and the University of Waterloo in Canada. We are working to develop advanced software security techniques that allow us to prove mathematically that critical components are secure. CHACE can help healthcare organizations comply with security and privacy rules set by HIPAA and other regulations.

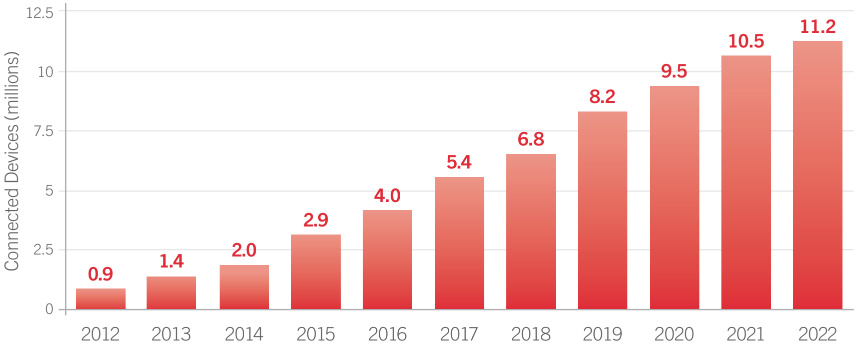
BlackBerry envisions a day when we can enable healthcare workers and patients to control life-critical healthcare devices such as wearable insulin pumps from their smartphones. No longer are we just worried about hackers getting ahold of our selfies; now we need to keep out hackers from breaking into devices that keep us alive. Currently, there is no standardized methodology that consumers, caregivers, insurance companies, and governments can use to determine whether a device is secure enough to be trusted for such a potentially dangerous use.

Telemedicine – Emerging A-P



Source: Machina Research

Telemedicine – World



Source: Machina Research

BlackBerry is aiming to help solve this problem and create cybersecurity standards for connected medical devices. Under the auspices of the Diabetes Technology Society, BlackBerry is part of a steering committee consisting of medical device manufacturers, caregivers, and representatives from Health Canada, the FDA, the National Institutes of Health, and the Department of Homeland Security.

BlackBerry's Healthcare Internet of Things

BlackBerry is the most trusted name in mobile security. We are using all of the tools at our disposal – our secure firmware stack from our QNX division, military-grade cryptography, communications protocols, and management services – to help IoT vendors design products that are safe and that can be managed remotely. So many of the hard problems relating to IoT security – for example, how to safely update software and policy over-the-air – we have already solved for mobile devices and are applying now to connected devices.

The Internet of Things will revolutionize the way that healthcare organizations treat, monitor and interact with patients. And as medical device manufacturers continue to evolve their products to take advantage of IoT, BlackBerry will be there to help protect patient safety and privacy.

David Kleidermacher is the Chief Security Officer for BlackBerry. David is responsible for the global Product Security organization, leading efforts to ensure BlackBerry's continued leadership in secure enterprise mobility. David is a world-renowned expert with deep experience in operating systems, high assurance software development techniques, mobile device security and the Internet of Things (IoT).

Smarter Healthcare: How Secure, Remote Management of IoT-Enabled Medical Devices Can Save Time, Money, and Lives

By Chris Ault, Senior Product Manager, QNX Software Systems

The medical devices we use in our hospitals and clinics today are due for an upgrade. It's not that they are necessarily bad at their core functions of delivering medicine, monitoring patients' vital signs, or jumpstarting hearts. Rather, the issue revolves around the important job of managing and maintaining these devices so that they can work properly, help patients, and save lives. Currently, the management and maintenance of medical devices requires clinical staff to do a lot of manual work. This not only requires extensive time from health providers and distracts them from providing actual patient care, but the sheer repetition of the manual maintenance work also introduces the possibility of human error.

Take the ubiquitous IV pump, for example. IV pumps are one of the most common pieces of equipment in hospitals, with at least one per patient bed. Indeed, the market for infusion pumps (including hospital ones, and those used for home healthcare and wearable insulin pumps) in the United States alone is expected to grow to $3.6 billion by 2017, according to the *Millennium Research Group* ➔.

However, IV pumps require regular maintenance by hospital staff to ensure that they work properly. This maintenance includes updating the database of drugs served by the pump to help make sure that patients get the right doses, and manually checking and replacing batteries, drugs and other consumables, parts that easily wear out, and so on.

In addition, conventional IV pumps cannot be programmed or easily automated today. For instance, I know of one hospital that has a dedicated hospital technician whose sole job all day, every day, is to update the drug libraries on the 900 IV pumps inside the hospital. The process is so laborious and time-consuming that it takes this worker a whole year to update all 900 IV pumps. By that time, it is time to repeat the whole Sisyphean cycle all over again.

Enter the Healthcare Internet of Things

The Internet of Things (IoT) describes the emerging class of gadgets and devices that are imbued with processing power and wireless networking capabilities formerly reserved only for computers. Just as the Internet made PCs so much more powerful, connected medical devices suddenly become smarter, more powerful, and easier to manage.

> A smart, connected IV pump can send alerts when it is low on drugs or when it needs to be updated, saving hospital staff valuable time.

> Surgical robots let doctors operate on patients thousands of miles away. But they must have hacker-proof security built in, lest they open a Pandora's Box.

What are the implications of a healthcare Internet of Things (IoT)? Let's go back to the example of the hospital technician updating the drug libraries on the hospital's fleet of IV pumps. With smart, connected IV pumps, the technician can update the drug libraries remotely, all at the same time. Suddenly, a job that took a whole year can be accomplished in a single day. In addition, an IV pump can send an alert to hospital staff when it is low on a particular medicine, rather than forcing caregivers to continually check each pump.

Making Defibrillator Malfunctions a Thing of the Past

Another scenario is automated external defibrillators (AEDs) located in public places that help save the lives of those people having heart attacks. The problem is that these devices are rarely used, so batteries and other parts can expire over time, or design flaws can be exposed, causing the AEDs to malfunction or fail during a crisis situation.

Such technical malfunctions likely contributed to more than 750 deaths in the five-year period between 2004 or 2009, according to the United States' Food & Drug Administration. The FDA received *approximately 72,000 reports of failed AEDs between 2005 and 2014* ➔. And since 2005, "manufacturers have conducted 111 recalls affecting more than two million AEDs," reported the FDA. In February 2015, the FDA issued an order to boost oversight and review of these devices to prevent those failures.

Remote management of AEDs can help improve these problems by enabling manufacturers or hospital staff to easily check on the remaining battery life of a defibrillator or be alerted when components are about to expire or malfunction. The AED's software and data can also be remotely patched and updated.

Preventing Problems

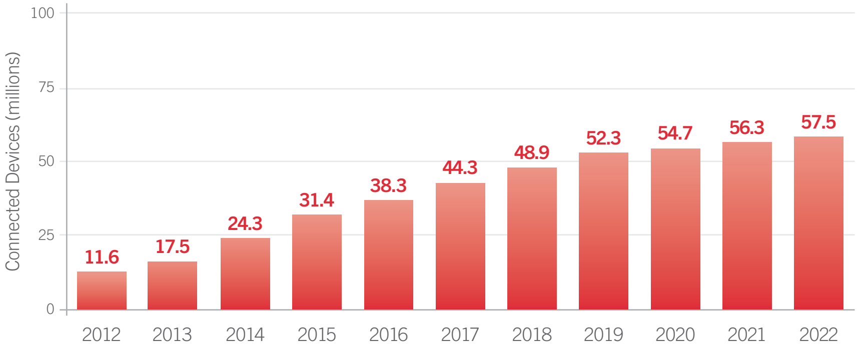
These are all advantages. However, one potential downside is that the IoT brings additional points of entry for hackers looking to steal patients' personal data or, worse, looking for ways to harm – or threaten to harm – patients hooked up to connected medical devices. Needless to say, security and rock-solid reliability are both key. The medical devices and the back-end management software with which they communicate must be constructed on secure, real-time platforms that can be made impervious to intruders or interruptions.

An example is medical telerobots that enable doctors to perform surgery remotely through the Internet. Such telesurgeries have been taking place since 2001. Medical experts consider this type of surgery as a boon for patients in parts of the world with a scarcity of trained surgeons.

But in *MIT's Technology Review magazine in April 2015*, security experts showed how vulnerable a telerobot may be to being hacked or disrupted in the middle of an operation.

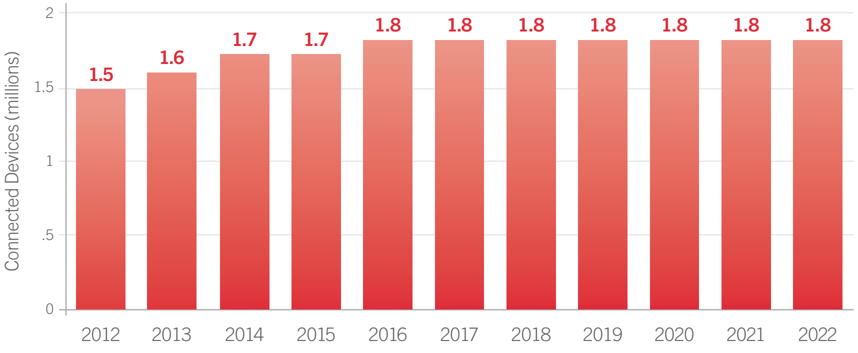
Enter BlackBerry, which brings proven realtime platforms for building tomorrow's connected medical devices and secure remote management software. For the former, the QNX® Neutrino® OS is a realtime operating system that is the most widely used by carmakers to build infotainment systems to date, with deployments in more than 60 million cars. QNX is also one of the few realtime operating systems with IEC 62304 compliance for use in Class III life-critical medical devices. QNX software is already used in a variety of medical devices, including a medical imaging machine used in surgery to show heart, arteries and veins, and several surgical robots used in precise, non-invasive surgery.

Connected Medical Environments – World



Source: Machina Research

First Responder Connectivity – World



Source: Machina Research

For the latter, BES®12 is the Enterprise Mobility Management (EMM) software used by tens of thousands of companies to securely manage their smartphones, whatever OS they run (including iOS®, Android™, Windows Phone®, and BlackBerry). On the BlackBerry roadmap is the ability to expand BES12 management capabilities to include a variety of devices, including medical ones.

The coming wave of IoT-enabled medical devices will deliver huge benefits to healthcare providers and patients alike. Besides saving lives, reducing errors and time, IoT-enabled medical devices will deliver cost efficiencies and ease management headaches that healthcare facilities will appreciate. However, those advantages are balanced by real potential security risks. Connected device manufacturers must build these preventative safeguards – and healthcare facilities using those devices must choose and enable them. Otherwise, we'll be opening a Pandora's Box that we will all regret.

Chris Ault is a Senior Product Manager at QNX Software Systems, a subsidiary of BlackBerry.

IoT Solutions Provide Crucial Tools to Address the Diverse Demands of the Healthcare Sector

By Andy Castonguay, Principal Analyst, Machina Research

There is no need to mince words. The truth is that healthcare is a complicated, messy business. Few business sectors are as complex and fragmented and yet remain as vital to society as healthcare. In a sector struggling to contain costs, facing heavy regulatory scrutiny, balancing scarce and inequitably distributed resources, and addressing the very real demands of sick patients, healthcare organizations are increasingly looking to new Internet of Things (IoT) technologies and approaches as potential solutions to many of these challenges.

While no IoT solution will offer a simple panacea for these myriad concerns, the fact is that today's IoT healthcare solutions can and do provide tangible benefits to healthcare organizations and their patients when designed and implemented well. But with an expanding array of IoT solutions to choose from, how should healthcare leaders and organizations best apply these new devices and capabilities of IoT solutions to address their key concerns and responsibilities most effectively? This chapter will propose a decision framework that healthcare organizations and leaders can use to analyze IoT solution value and viability.

Whether adding purpose-built IoT solutions to a department or weaving together solutions into a comprehensive architecture, healthcare organizations should benchmark potential solutions against a comprehensive matrix to assess whether new technologies and solutions will justify the financial investment and organizational commitment needed to get it up and running. At Machina Research, we believe the Internet of Things is not a specific technology, but rather an architectural framework that can and should integrate multiple technologies and datasets, facilitate critical analytics and enhance performance.

Within the healthcare sector, "performance" is often viewed through a multi-faceted lens, combining medical outcomes, cost efficiency and other factors. The one consistent non-negotiable requirement of IoT solutions is that they ensure a high level of security related to the integrity of and access to patient data. Hospital IT leaders will need to design their systems to guarantee data security across multiple platforms and among multiple partner organizations and vendors. Beyond the foundation of privacy and security, most medical IoT solutions are designed for a specific purpose, but ideally a well-designed IoT solution will positively address two or more of the following core considerations and therefore elevate the overall performance of the medical practice:

Healthcare IoT Decision Matrix

Core questions for the assessment of new IoT solutions

Will the IoT solution lead to demonstrably improved health outcomes?

Will the IoT solution notably increase operational revenues and margins?

Will the IoT solution expand the addressable continuum of medical care and/or operational capabilities?

Will the IoT solution enrich patient engagement?

Will the IoT solution facilitate greater integration and interoperability with service partners and/or create a tangible competitive advantage?

In the diverse healthcare arena, it is most likely that each organization will establish its own ranking or weighting for these key questions. In fact, few well-designed IoT healthcare solutions address only one of these key issues. Keeping in mind the idea of a broader IoT framework, indeed, a well-deployed IoT architecture will integrate data from a diverse set of sensors, devices, machines, databases and software platforms to facilitate careful analysis and improved performance. In the following sections, we will highlight several examples of commercially available IoT solutions and approaches that are already facilitating gains in medical and operational performance and, in some cases, extending the addressable market and revenue opportunities for leading-edge organizations.

Leveraging IoT solutions for improved patient outcomes

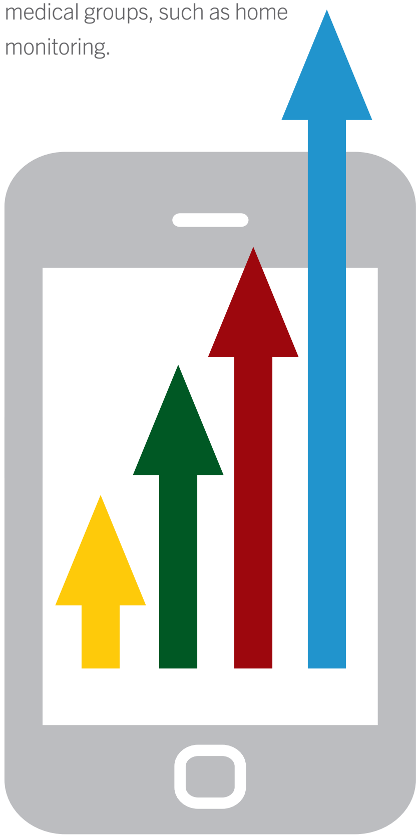
For many IoT healthcare solutions, improved patient outcomes are paramount to the design and function of the solution. From a decision matrix perspective, for patient-facing IoT solutions, improved outcomes should be a clear priority, especially when the solution and its data outputs can be used in concert with a medical facility's healthcare records platform, medical workflow systems and trusted third-party service partners. IoT-enabled clinical measurement devices permit the monitoring of a patient's vital signs with increased frequency and accuracy well beyond the traditional physical limits of medical facilities. With increased frequency of readings combined with timely data analysis, patient monitoring gains great consistency and patient data can become more usable in real time, helping to avert adverse healthcare events. Combining detailed health record analysis and around-the-clock patient monitoring as part of its Telesepsis initiative, Mercy Hospital in St. Louis, Mo., reported decreasing septic shock-related deaths from 46.7 percent to 18.5 percent and reducing the average length of stay in the intensive care unit from 8 to 3.4 days, within the first 11 months of the program.

Utilizing IoT solutions to enhance operational revenues and margins

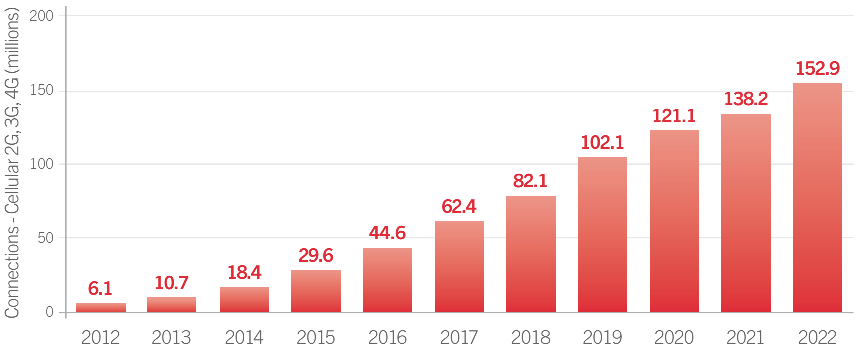
One of the most promising implementations of IoT technology is the integration of sensors and connectivity to monitor and maintain hospital equipment. Manufacturers of hospital equipment and their medical customers can benefit from remotely monitoring the performance of individual pieces of equipment and components, in order to support preemptive maintenance and remote problem diagnosis/resolution as part of value-added services. Through these design and process improvements, medical device manufacturers can reduce the frequency of on-site repairs while also gaining the facility to shift maintenance visits increasingly to non-operational hours, thus reducing service disruptions for clients and permitting increased uptime for medical devices and machines.

Extending the continuum of care and operational capabilities through IoT solutions

Through IoT-enabled treatment and monitoring equipment, clinical care will increasingly become a reality in patient homes. With dynamic monitoring systems to track their health, safety and activities, seniors can stay in their homes longer, improving their comfort and minimizing cost of care. In addition to the patient benefits, medical organizations that develop dynamic and efficient service platforms can also begin to offer these services to other medical groups, such as home monitoring.

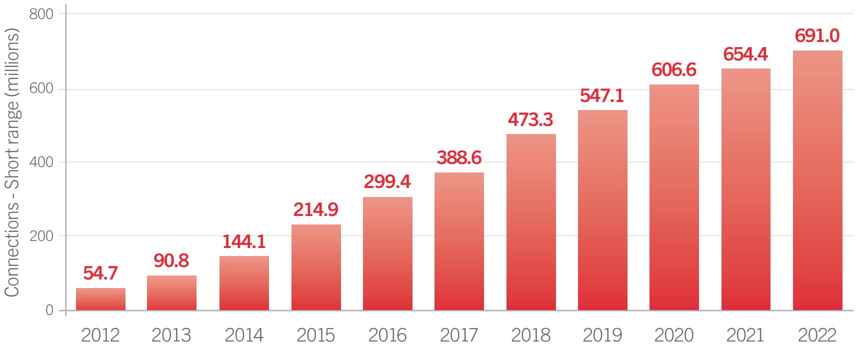


Connected Device Connections (Cellular 2G, 3G, 4G) — World



Source: Machina Research

Connected Device Connections (Short Range) — World



Source: Machina Research

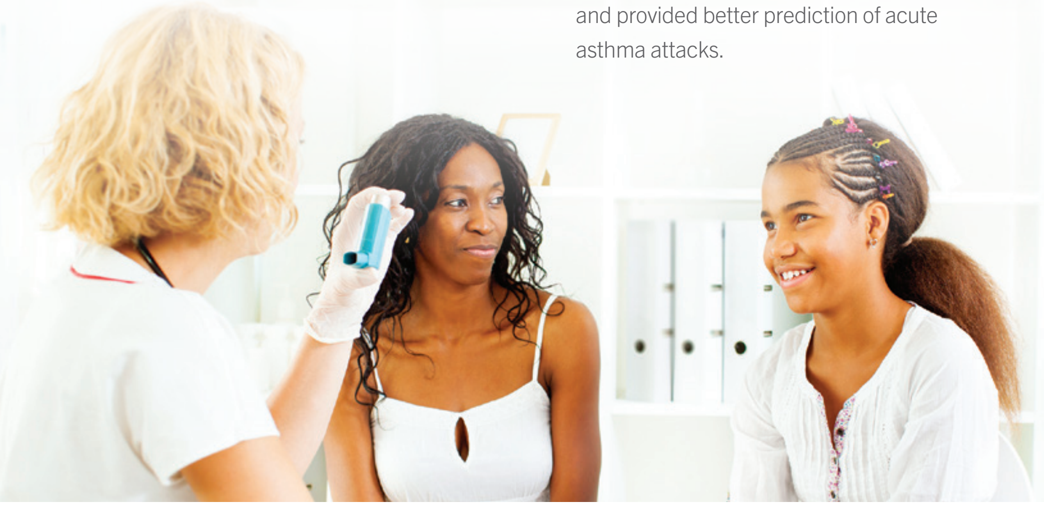
Beyond extending health services into the home, new IoT eHealth/mHealth solutions are expanding the geographic reach of medical services to include remote communities and even international consultations. Historically, conventional telemedicine solutions allowed patients living in remote regions to gain access to medical providers through telephone, video conferencing and remote diagnostics. Through improved, secure video conferencing and lower-cost, connected diagnostic equipment, eHealth/mHealth is permitting physicians to reduce travel and in-office patient appointment cancellations.

This combination is allowing doctors to greatly increase the number of patients they can "see" in a day and facilitate a more convenient experience for their clients. Some doctors interviewed by Machina Research report doubling their patient loads while also opening up their practice to other geographies, both domestic and international. For Stanford Medical in California, high-definition video conferencing and remote diagnostics have not only allowed specialists to treat more patients in more remote Northern California communities, but has also become a vehicle to serving affluent Chinese in Shanghai, leveraging the facility's reputation and technology adoption to attract new clientele.

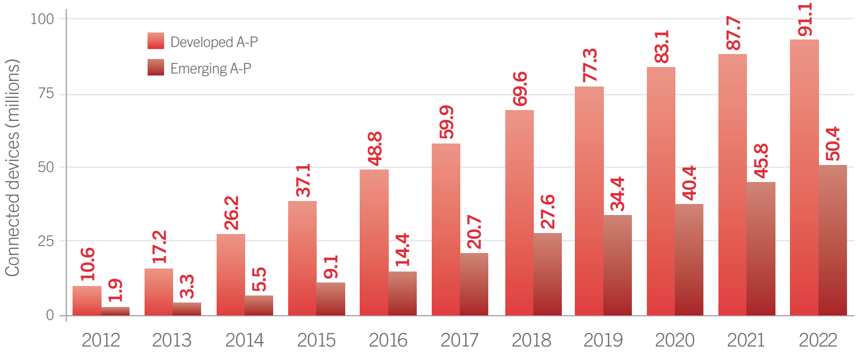
Designing IoT solutions for improved patient engagement

With effective management of smartphones, tablets and computers used by medical professionals and integration of IoT device data, medical systems can gain great consistency and change the nature of patient engagement. With wearable monitors and sensors in the home gathering essential data in a consistent fashion, physicians and nurses can spend more time assessing behavioral, environmental and other contributing factors to patient health problems.

IoT solutions that use consistent patient monitoring in and out of the hospital introduce a new paradigm for assessing and improving patient compliance with physician orders and prescriptions. Through enhanced patient engagement applications linked to IoT sensors and devices, medical providers can reduce the recidivism of patients to emergency rooms and medical facilities. The leading edge of connected blood glucose meters, asthma inhalers, connected prescription pills, and other innovative products can establish a clear record of patient compliance through device data and engage patients through smartphone applications to offer guidance, education and support for improved self-care and related behaviors. Propeller Health's smart inhaler system monitors patient usage of asthma medication while also interacting with the patient through a smartphone application to influence behavior. In early trials, the combination of monitoring and engagement has led to an 80 percent improvement in medication compliance among asthma patients and provided better prediction of acute asthma attacks.



Connected Device Growth — Developed A-P and Emerging A-P

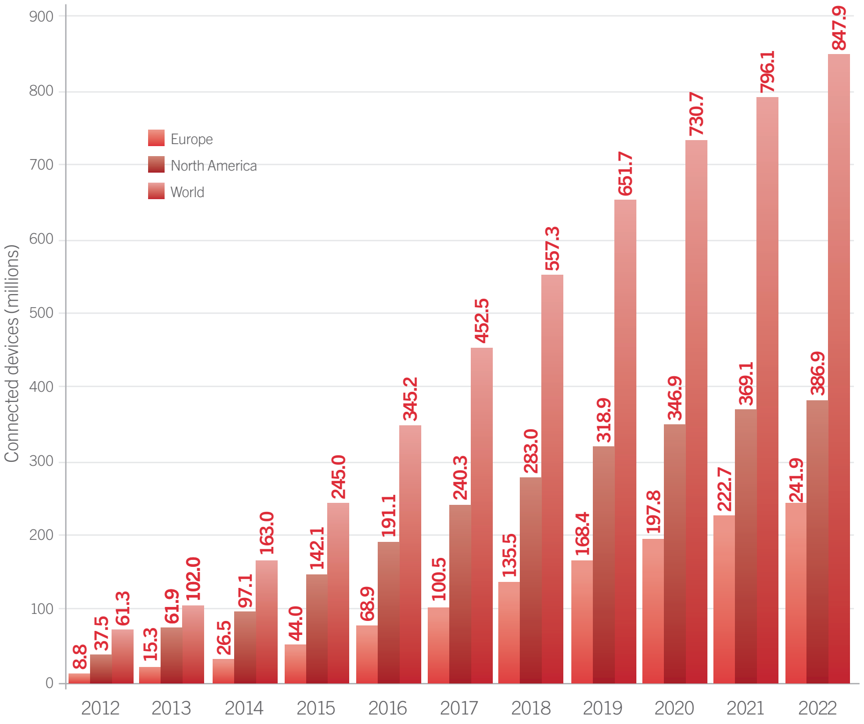


Source: Machina Research

Establishing competitive advantage through IoT implementations

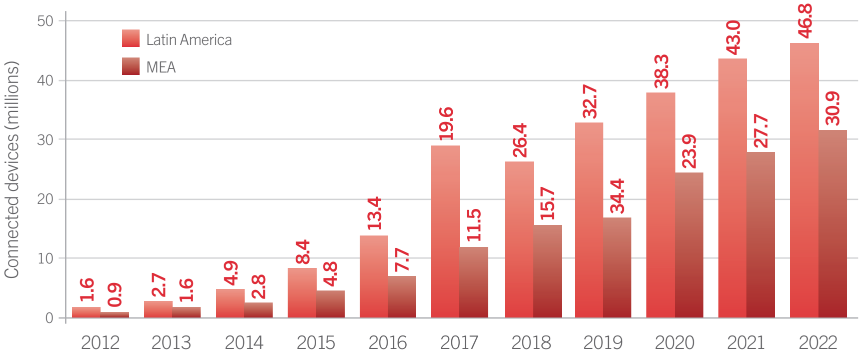
Perhaps the single most important insight into healthcare-related IoT is that dynamic new solutions are poised to disrupt and alter conventional healthcare delivery business models throughout the continuum of care. For executives and strategic leaders within the medical community, there will be an increasing imperative to expand and defend their existing business. A key example is new approaches to reducing the time necessary to schedule an appointment with a primary care physician. A *2014 study by Merritt Hawkins* ❯ showed that on average, patients in the U.S. must wait 19 business days before they can schedule a visit with their doctor.

Connected Device Growth — Europe, North America and World



Source: Machina Research

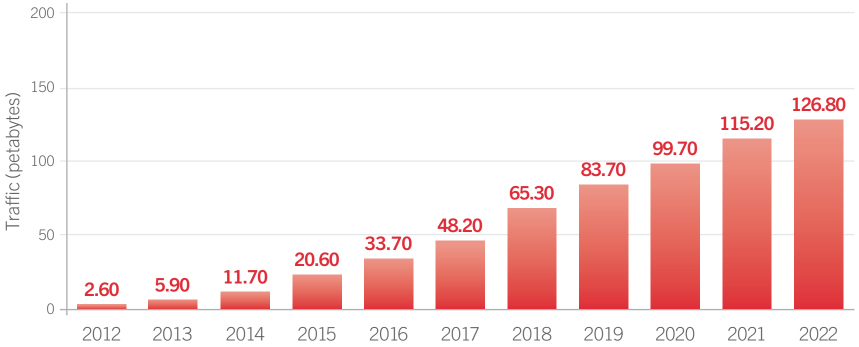
Connected Device Growth — Latin America and MEA



Source: Machina Research

With health insurance companies beginning to offer medical triage through secure video conferencing and companies like HealthSpot providing medical consultations in IoT-enabled diagnostic pods co-located in pharmacies, conventional business models related to medical services access are being threatened from multiple angles. While this particular disruption trend is still in its early phases, organizations that quickly establish leadership and provide a compelling and convenient medical services access model will be best positioned to attract and maintain patient loyalty. With new healthcare start-ups offering reasonably priced concierge physician services, in-home physical therapy using video and software, and other innovative business models, traditional healthcare facilities will need to consistently evaluate competitive risk. More importantly, these organizations will need to leverage IoT healthcare solutions to establish their own competitive advantage within an increasingly competitive medical services landscape.

Connected Device Data Traffic Growth – World



Source: Machina Research

Conclusion

Although connected devices, machines and remote monitoring equipment have played a role in healthcare for many years, the advent of the Internet of Things into the healthcare community represents a new stage of connected healthcare. The adoption of IoT and its potential for linking diverse assets and devices across the continuum of care will challenge healthcare executives to look at their IT and software platform strategies with critical new eyes.

In a broader context, healthcare organizations will need to recognize that the age of buying standalone, point solutions is quickly coming to an end, technologically speaking, and that future efficiencies and indeed improved patient outcomes will be dependent on how well an organization embraces and manages a complex set of connected assets and data streams across its own plant(s) as well as those of partner organizations and patient environments. Prescient healthcare companies will recognize that IoT solutions hold the power to help drive improvements as well as be a vehicle for potential disruptions to their core business models, and therefore develop IoT strategies that focus on improving patient outcomes, improving operational efficiency and establishing the organization as a core services partner for the broader healthcare community.

Andy Castonguay is a Principal Analyst at Machina Research focused on the rapidly evolving M2M and IoT ecosystems in the Americas with particular focus on mobile health solutions and the M2M devices space. With over 15 years of experience in Latin America and North America, Andy has worked extensively with mobile network operators, device manufacturers, technology vendors, and financial institutions in both mature and growth markets.

List of Sources

Berg Insight, *mHealth and Home Monitoring*, 2013

BlackBerry, *BlackBerry Customer Success Stories*

BlackBerry, *The Definitive Guide to Enterprise Mobile Security*

BlackBerry, *Mobility Risk Tolerance Survey*, 2014

Communications and Electronics Security Group (CESG), *End User Devices Security and Configuration Guidance*, 2015

eWeek, *Top Mobile Apps Overwhelmingly Leak Private Data: Study*, 2013

Forrester Research, *Brief: Stolen And Lost Devices Are Putting Personal Healthcare Information At Risk*, 2014

Forrester Research, *Forrsights Telecom And Mobility Workforce Survey, Q2 2013*, 2013

Forrester Research, *Mobile Healthcare's Slow Adoption Curve*, 2011

Gartner, Inc., *Bring Your Own Device: The Facts and the Future*, 2013

Gartner, Inc., *Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration*, 2014

Gartner, Inc., *Protecting Enterprise Information on Mobile Devices, Using Managed Information Containers*, 2014

Gartner, Inc., *The Impact of Mobility on the IT Service Desk*, 2013

Health Leaders Media, *The Transformation of Healthcare Delivery*, 2015

Home Care Pulse, *Private Duty Benchmarking Study*, 2015

IDC, *Worldwide File Synchronization and Sharing 2014-2018 Forecast and 2013 Vendor Shares*, 2014

Joint Commission, *Sentinel Event Data, Root Causes by Event Type*, 2012

Journal of Neurology, *Tablet computers with mobile electronic medical records enhance clinical routine and promote bedside time: a controlled prospective crossover study*, 2015

KPMG, *Healthcare Cybersecurity Survey*, 2015

Machina Research

Medscape, *The Inhospitable Hospital: No Peace, No Quiet*

Merritt Hawkins, *Physician Appointment Wait Times and Medicaid and Medicare Acceptance Rates*, 2014

Millennium Research Group, *US Infusion Pump Market To Grow Strongly To $3.6 Billion By 2017*, 2012

MIT Technology Review, *Security Experts Hack Teleoperated Surgical Robot*, 2015

National Institutes of Health, *mHealth – Mobile Health Technologies*

Office of the National Coordinator (ONC) for Health Information Technology, *Connecting Health and Care for the Nation: Nationwide Interoperability Roadmap*, 2014

Office of the National Coordinator (ONC) for Health Information Technology, *Individuals' Perceptions of the Privacy and Security of Medical Records*, 2015

Ontario Hospital Association, *Hospital Support Workers study*, 2001

Ovum, *2015 Trends to Watch: Enterprise Mobility report*, 2014

Ovum, *Beyond BYOD: How Businesses Might COPE With Mobility*, 2014

Ovum, *New mobile workspaces and the business value of a shift to user-centric computing*, 2014

PLOS ONE, *The Influence of the Patient-Clinician Relationship on Healthcare Outcomes: A Systematic Review and Meta-Analysis of Randomized Controlled Trials*, 2014

Ponemon Institute, *Cost of Data Breach Study: Global Analysis*, 2014

Ponemon Institute, *Fifth Annual Study on Privacy & Security of Healthcare Data*, 2015

Ponemon Institute, *The Imprivata Report on the Economic Impact of Inefficient Communications in Healthcare*, 2014

PricewaterhouseCoopers Health Research Institute, *Healthcare Unwired*

SANS Analyst Program, SANS Institute, *New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations*, December 2014

Spyglass Consulting, *Point of Care Communications for Nursing*, 2014

Spyglass Consulting, *Point of Care Communications for Physicians*, 2014

Tractica, *Home Health Technologies*, 2015

U.S. Food and Drug Administration, *FDA takes steps to improve reliability of automated external defibrillators*, 2015

VDC, Enterprise Mobility Service Survey, 2006

VDC, *Wireless Home Care Solutions: Addressing the Quality of Service and Performance Gap*, 2007

BlackBerry.com

IMPORTANT: Results provided for informational purposes only and will vary depending on the individual customer and the specific operating circumstances. This material, including all material incorporated by reference, is provided “AS IS” and “AS AVAILABLE” and without condition, endorsement, guarantee, representation or warranty of any kind by BlackBerry and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors or omissions in this material and shall not be liable for any type of damages related to this material or its use, or performance, or non-performance of any software, hardware, service, or any references to third-party sources of information, hardware or software, products or services.

©2015 BlackBerry Limited.