Emerging Technology Series

Mobile Computing in Clinical Settings

Using mobile devices to obtain seamless extension of the health enterprise's digital ecosystem

White Paper (Full Report)

Canada Health Infoway
Inforoute Santé du Canada

November 2013

1. Disclaimer

This white paper represents solely the views of Canada Health Infoway (*Infoway)*. It is based on *Infoway's* research and analysis as well as information from various sources. *Infoway's* views are based on information and analysis which *Infoway* believes is sound and reliable, as of the publication date of this white paper.

This white paper is informative only and cannot be interpreted as providing any indication of *Infoway's* present or future strategies or investment criteria.

This white paper is provided as is. No representation or warranty of any kind whatsoever is made by *Infoway* as to the accuracy, infringement of third party intellectual property, completeness, fitness for any reader's purpose, or correctness of any information or other contents contained in the white paper, and *Infoway* assumes no responsibility or liability if there is any inaccuracy, infringement of third party intellectual property, incompleteness, failure to meet any reader's purpose or incorrectness with respect to any of the information or other contents contained in the white paper.

Infoway does not assume any responsibility or liability related directly or indirectly to the white paper, including without limitation with respect to any person who seeks to implement or implements or relies or complies with any part or all of the ideas, recommendations or suggestions set forth in the white paper.

Infoway does not implicitly or explicitly endorse any particular technology or solution of any vendor or any other person, it does not guarantee the reliability or any proposed results related to the use of such technology or solution and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the white paper.

Infoway does not make any implicit or explicit commitment of any kind or nature whatsoever to make any investment in any particular technology or solution, and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the white paper.

Anyone using the enclosed material should rely on his/her own judgment as appropriate and seek the advice of competent professionals and experts.

© Canada Health Infoway Inc. 2013

This white paper is the sole and exclusive property of *Infoway* and *Infoway* reserves all intellectual property rights, including but not limited to copyright.

Table of Contents

2. Executive Summary

This white paper covers the effective use of mobile devices in health care by clinicians and its relevance for the digital health community in Canada. It provides clarification on the definition and characteristics of mobile health (mHealth), its economic value, the privacy and security considerations, some of the operational considerations and *Infoway's* view on opportunities for its effective application in the Canadian digital health and health care delivery context. This white paper does not attempt to cover applications and devices that address personal health and fitness used by consumers.

Smartphones and tablets have ushered in transformations for consumers and businesses in terms of communications and process efficiencies. Smartphones have emerged with capabilities that far exceed making phone calls, using email, and even access to web-based applications. More than one in every two adults in Canada now owns a smartphone with adoption rates significantly higher among younger adults. Mobile devices surround us with information that moves with us. Smartphones and tablets can go places where a personal computer (PC) or even a laptop cannot, and thereby create new opportunities for productivity gains in health care.

Approximately two years ago, the late Steve Jobs, Apple CEO, declared that we had entered the post-PC era when the sales of smartphones began to outnumber desktop PC sales. Consumers, including clinicians, have been increasingly trending their purchase decisions away from laptops and toward tablets. In the U.S. alone, Forrester expects that tablet sales will grow from 10.3 million in 2010 to 44 million in 2015, surpassing laptop sales by roughly five million units.

Major Technological Shift Underway in Medicine

Outside of the implementation of electronic health records (EHRs), the use of mobile devices promises to be one of the most transformational information technologies in health care. Clinicians want a highly useful, portable and convenient tool to use in their practice – one that will improve workflow and become a handy channel of connectivity to applications and information assets. Mobile devices meet this need by enabling clinicians to practise medicine from anywhere and at any time.

The use of smart devices is one of several key enablers that *Infoway* believes can address the important challenges facing health care systems, such as the need for greater cost and process efficiencies in the delivery of care. Functions that were not possible without the mobile platform are now available for deployment and include real-time monitoring and alerts using wireless devices and sensors. These mobile solutions can inform clinicians on the status of their patients' diagnostics, health states, behaviours, activities and medication compliance.

Many of the functions that can be performed using PC-based clinical information systems are being ported to mobile platforms that allow on-the-move clinicians new channels and flexibility for completing routine tasks such as:

- communicating with colleagues
- accessing patient health records including diagnostic and radiological images
- consulting reference sources such as drug formularies and dosing guidelines, clinical practice guidelines and Health Delivery Organization (HDO) policies
- Computerized Physician Order Entry (CPOE)[1]
- clinical documentation.

New Challenges

The growth in mHealth does introduce important challenges that HDOs will need to consider, such as: how will their clinicians sort through the tens of thousands of available mHealth apps to find the most appropriate solution for their professional needs? How will clinicians respond to questions from their patients about the appropriateness of certain health apps? When and how will clinicians validate the quality of health apps' interoperability, privacy, security and content features?

The small form factor of smartphones and tablets is a key driver for their use in health care. However, it makes these devices strong candidates for misplacement, loss or theft. The primary concern with mobile device loss or theft is the access to confidential information either stored on the device or accessed by the device. The new challenge introduced by mobile devices relates to authentication of individuals accessing personal health information wherever it is located.

As with the use of other devices, there are also infection prevention and control risks to be aware of with the use of mobile devices in health care settings. Smartphones and tablets are at risk of becoming carriers for the transmission of microorganisms as they travel with clinicians into virtually every environment and from patient to patient. The challenge will be to raise awareness among clinicians about the infection control risk and to guide their behaviour with respect to infection prevention and control through education, training, and policy tools.

[1] For the purpose of this white paper, the definition of CPOE is meant to include physicians and all providers who may initiate orders. See for reference: http://en.wikipedia.org/wiki/CPOE

Clinicians as Consumers and the Need for Governance and Strategy

Clinicians and health care employees are behaving like consumers by wanting to exercise choice over mobile device and app selection. In response, some organizations are adopting management and ownership models such as "bring your own device" (BYOD)[2]. In such cases, new tools, architectures and policies are needed to govern and control these endpoint devices.

Health delivery organizations run the risk of not planning and managing their mHealth initiatives in a strategic or proactive approach. Many mobile expansions can be fragmented with overlapping approaches to planning, procurement, governing policy, application design and end user support. *Infoway* recommends that HDOs think through their mobile computing strategy in context with their other digital health investments such as hospital information systems (HIS), electronic medical records (EMRs), EHRs and health analytics.

Promised Value

As typical of new technologies, there has been a lot of hype and promise surrounding the capabilities and benefits of the use of mobile devices in health care delivery. For example, a common claim is that clinician productivity increases with the use of mobile health technologies.[3]

Several multinational consultancies have recently completed mHealth studies forecasting the benefit impact on the health care system. These studies predict that mHealth technology with its many functions will maximize health care professionals' time by speeding up processes, reducing the possibility for human error, avoiding duplication, and enabling remote access to centralized electronic health records. One study predicted that mobile devices can reduce the administrative burden of health care delivery for clinicians by 20 to 30 per cent.[4] Another study found that approximately two-thirds of physicians reported increased productivity with the use of mHealth applications in the hospital setting.[5]

---

[2] Wikipedia defines Bring Your Own Device (BYOD) as *"the recent trend of employees bringing personally-owned mobile devices to their place of work, and using those devices to access privileged company resources such as email, file servers and databases as well as their personal applications and data."*

[3] mHealth in an mWorld: How mobile technology is transforming health care, Deloitte, 2012.

[4] The Socio-Economic Impact of Mobile Health, Boston Consulting Group/Telenor Group, April 2012.

[5] mHealth in an mWorld: How mobile technology is transforming health care, Deloitte, 2012.

Clinicians deploying mHealth technologies to their patients can also achieve efficiencies. In the U.S., Veterans Health Administration (VHA) clinicians have deployed mobile monitoring devices to thousands of their chronically ill patients at risk for institutional care. The VHA has reported reductions in bed days of care in excess of 40 per cent for their home telehealth enrolled patients.[6] A recent Canadian assessment of the economics of home telemonitoring for patients with various chronic diseases indicated reductions in: number of hospitalizations; average length of inpatient hospital stay; and emergency room visits.[7]

A Call to Action

Mobile technologies are being introduced to the health sector with much promise. In spite of the lack of empirical evidence of its efficacy at scale, many HDOs are embracing mobile health capabilities.

Infoway's view is that mHealth is more than an emerging set of technologies. We believe it should be regarded as a priority component of the health enterprise's IT strategy and supported as a platform.

We encourage HDOs to:

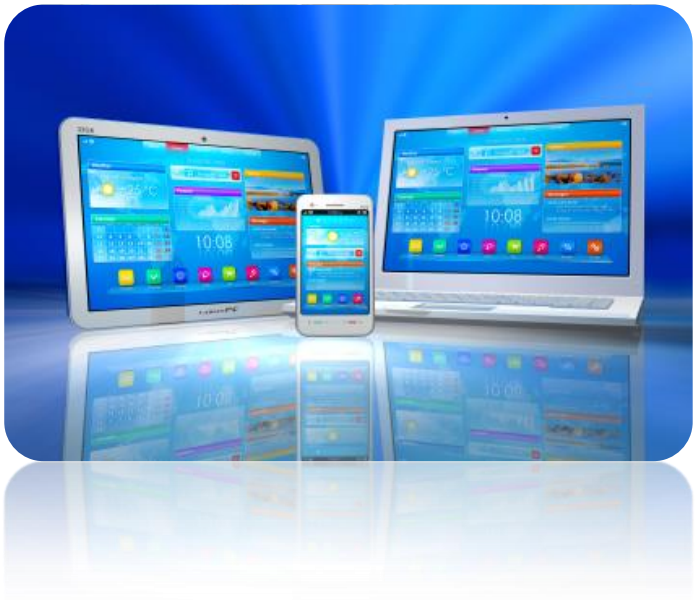
1. Appoint an executive sponsor and expand scope of IT governance to provide oversight for mobility, alignment with business goals, and integration into all parts of the enterprise.
2. Develop a mobile strategy that is integrated into the broader health information and communications technology strategy roadmap.
3. Deploy mobile devices to their clinical staffs (or support a BYOD model) in alignment with the enterprise's business strategy.
4. Consider that future software solution deployments which support clinicians include a mobile user interface option (to multiple mobile platforms where required).
5. Invest to achieve seamless integration of mobile devices across the health enterprise's information and software services assets and effectively into its digital health ecosystem.
6. Create a set of policies and standards within a regulatory framework that directs the management and use of privacy-enhanced mobile devices and apps by clinicians and staff.
7. Consider the use of curation services for medical devices and mobile apps to assist clinicians to source and prescribe these solutions to their patients.

---

[6] Broderick, M. et al, Scaling Telehealth Programs: Lessons from Early Adopters, Commonwealth Fund pub. 1654, Vol. 1

[7] Home Telemonitoring for Chronic Disease Management: An Economic Assessment, HEC Montreal, August 2012.

Infoway notes that clinicians are embracing mobility and in some organizations are champions leading their colleagues forward. *Infoway* is confident that mobile devices and apps will continue to evolve and become valued and trusted clinical tools just as the stethoscope has been for nearly 200 years.



This white paper provides additional insight into mHealth, opportunities for its effective application by clinicians in the Canadian digital health and health care context, and identifies risks and challenges associated with its use.

3.Introduction

The term mobile health (mHealth) has become very visible as a new capability of information management within health delivery organizations (HDOs) such as hospitals, clinics and physician practices. It refers to the use of mobile and wireless devices to improve health outcomes, health care services and health research. While some technologies and capabilities underlying mobile telecommunications have been in existence for the past couple of decades, the use of mHealth technologies by clinicians has just recently begun to transform HDOs. For the purposes of this paper, *Infoway* is including remote patient monitoring (e.g., wireless sensors and monitors deployed in the patient's home as directed by their clinician) within scope of its mHealth investigation.

This white paper covers the effective use of mobile devices in health care by clinicians and its relevance for the digital health community in Canada. It provides clarification on the definition and characteristics of mHealth, its economic value, the privacy and security considerations, some operational considerations and *Infoway's* view on opportunities for its effective application in the Canadian digital health and health care delivery context.

This white paper does not attempt to cover other perspectives of mobile devices used as diagnostic tools, use of wireless technologies such as Personal Emergency Alarm Systems, or radio frequency identification (RFID) tracking. Nor does it cover the use of mobile devices and applications that address personal health and wellness, such as fitness and diet, which are marketed directly to consumers.

The introduction of digitally connected mobile devices promises to deliver attractive benefits to patients, clinicians and health delivery organizations. *Infoway* believes that the greatest value from mobile device use will be realized when authorized clinicians can seamlessly access local, regional and provincial patient data repositories, streaming patient monitoring data and advanced services such as health analytics and clinical decision support, to perform functions just as they would traditionally do using a hospital or office workstation.

Given the popularity of smartphones and tablets and their potential for professional use, it isn't surprising that mHealth solutions are among the top information technology priorities for HDO chief information officers (CIOs) and chief medical information officers (CMIOs). Several Canadian HDOs have formal programs to meet the need for mobile computing among their clinicians. However, for many of these early adopters, interoperability with patient data repositories and access to software services is still limited. As such, the realization of benefits hasn't yet reached its potential.

A key challenge facing HDOs is the rapid increase in the number of new users, especially clinicians, whose adoption of mobile technology for professional purposes has often outpaced the rate of change at the IT enterprise level. In addition to the demands placed on the enterprise's IT services, this paper highlights important considerations for the effective use of mHealth devices including data governance, human resource policies, and other business processes, to mitigate the risks common to mobile device use in health care delivery.

Additionally, this paper discusses mHealth deployment models and implementation considerations including architecture, interoperability changes to applications to support multi-channel interfaces, mobile device management, and approaches for the privacy and security of personal health information.

4. Mobile Health

The capabilities of the mobile technology paradigm such as the smartphone have been in existence since 2000. However, mHealth has only very recently emerged as a transformative information technology in health care. Mobile device adoption is evolving quickly from its origins in the consumer market. In fact the tablet and associated apps, a favourite form factor with clinicians because of its size, simplicity and portability, did not exist prior to April 2010 when Apple released its first generation iPad.

The term "mHealth" will disappear as mobile device use becomes ubiquitous in health service delivery.

Clinicians have been the leaders of the mobility movement within health delivery organizations. Their scheduled activities and workflows require them to be in virtually constant motion within and outside of the health enterprise. To effectively practise, clinicians require the most up-to-date clinical information for their patients, frequent access to online medical references, near continuous communication with team members, and regular interaction with specialist consultants. Not surprisingly, clinicians are bringing media tablets and smartphones into the health enterprise in greater numbers. Many have enthusiastically embraced mobile devices to meet their needs in ways that stationary PCs, a computer on wheels and even laptops cannot.

The uptake of mobile devices has been impressive:

- 67 per cent of Canadian family physicians own a smart phone[8]
- 82 per cent use them for drug references[9]
- 50 per cent use them for clinical decision support[10]
- 30 per cent own an iPad, with the majority (62 per cent) using it for professional purposes[11].

The introduction of mobile devices to the health enterprise, particularly devices personally owned by clinicians and used for professional purposes, introduces important challenges and considerations that must be understood and addressed.

4.1 mHealth Defined

Gartner, an information technology research and advisory company providing technology related insight, describes mHealth as being similar to e-health in that it is a

[8] Prizm Healthcare Intelligence, March 2012.

[9] Ibid.

[10] Ibid.

[11] Manhattan Research: Taking the Pulse v11.

broad and nebulous concept that emphasizes the means (mobile device technologies and apps), not the end (actual use of mobile technologies in health care delivery). Gartner believes that as mobile technologies become incorporated into health service delivery, the term "mHealth" will become obsolete.

Infoway also believes that mobile and health technologies will converge in the next few years. There will be much less distinction between information (analytics), cloud computing, mobile and social media. They will all be highly integrated, intertwined and co-dependent components of the digital health ecosystem. Gartner has identified this convergence of technologies as the "Nexus of Forces" and believes that it will be so transformative as to replace current business models and technology architectures.

In the interim, *Infoway* asserts that clinicians are less concerned with the choice of mobile device or platform than they are with having convenient access to patient information, team members and reference resources wherever and whenever needed. In this regard, *Infoway* believes their expectation of the mobility movement is to seamlessly interact within their health ecosystem irrespective of whether they are using a laptop, PC or a mobile device.

Several prominent organizations, including the World Health Organization, have created definitions for the term mHealth. For the purpose of this paper, we offer the following definition.

The mHealth Alliance:

"Mobile Health, or mHealth, can be defined as medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, tablets, personal digital assistants and other wireless devices. The ubiquity of mobile devices in both developed and developing countries presents an opportunity to improve health outcomes through the innovative delivery of health services and information.[12]

4.2 Mobile Device Defined

A definition sourced from Wikipedia is as follows: *"a mobile device (also known as a handheld device, handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds (0.91 kg)."*[13]

For the purpose of this paper, *Infoway's* analysis focuses on handheld devices such as tablet computers and smartphones that are equipped with cellular, 3G, LTE, Wi-Fi and/or Bluetooth to allow connections to a corporate network, the Internet and other Bluetooth capable devices. We also include discussion on remote patient monitoring

[12] As accessed from: http://www.mhealthalliance.org/about/faq#

[13] As accessed from: http://en.wikipedia.org/wiki/Mobile device on October 9, 2013.

(e.g., wireless sensors and monitors that have been deployed to the patient's home at the direction of a clinician).

4.3 Mobile App Defined

A definition sourced from Technopedia.com is as follows: *"a mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer."*[14] For the purpose of this paper, *Infoway's* analysis focuses on apps that support functionalities such as data collection, health analytics such as decision support, and health monitoring.

Mobile devices also have the capability to run browser based applications similar to PCs. Browser based applications are common in the mHealth space especially when providing access to existing applications and services that are already web enabled. These types of applications typically do not use mobile device specific capabilities or information presentation tools and do not store information collected on the mobile device. The use of new protocols such as HTML5 will, over time, allow web based apps to offer similar functionality to those found in mobile apps (e.g., touch screen access, storing of information on mobile devices, access to location data).

4.4 Mobile Health Ecosystem and the EHR

Infoway recognizes that digital health ecosystems are beginning to evolve across the country. Many initiatives, such as an HDO enabling its clinicians to view patient records from mobile devices, have created new business value albeit with limited integration, and limited functionality to the enterprise's full information assets.

The evolution of a digital health ecosystem will require a collaborative of users from HDOs, pharmacies and labs, and a host of other actors including technology providers, content suppliers, telecom carriers, digital health organizations, and certification and regulatory agencies. For providers, HDOs and governments, the future state goals include system efficiencies and patient centred models of care enabled by supportive policies and mobile solutions that interoperate with local, regional and jurisdictional clinical data repositories.

Similar to the features of an EHR solution, the goal of developing a vibrant mHealth ecosystem is the creation of seamlessly connected clinical and business applications through the integration of mobile devices, communications and transactions.

[14] As accessed from: http://www.techopedia.com/definition/2953/mobile-application-mobile-app on October 9, 2013.

5. Major Technological Shift Underway in Medicine

It was estimated that there were 10.5 million smartphone users in Canada at the end of 2012.[15] Smartphone penetration is nearing half of all mobile users at 47 per cent, a significant increase over 2011, when 34 per cent of Canadians reported using such a device.[16] Tablet device use has also experienced impressive year-over-year growth with 21 per cent of Canadians reporting use of these devices in 2012, compared to 10 per cent in 2011.[17]

Outside of the implementation of EHRs, the use of mobile devices promises to be one of the most transformational information technologies in health care. Mobile devices such as smartphones and tablets have emerged with capabilities that far exceed phone calls, email, and even access to web applications. Mobile devices surround the user with information and can go places where even a laptop may not be able to, thereby creating new opportunities for productivity gains.

Dr. Eric Topol, an American cardiologist and geneticist who was named "Doctor of the Decade" by the U.S. Institute for Scientific Information, believes that a super convergence is underway to digitize the individual and that it will revolutionize health care. Topol believes that social networking, mobile devices and genomics powered by cloud based supercomputing will give consumers control over their individual information, which can be used in highly effective ways to protect health, manage illness and even prevent illness. Topol also believes that a new kind of doctor-patient relationship needs to emerge to take advantage of the information and technology savvy consumer. He argues that the physician's role should be to process the information with the patient, and provide guidance, judgment and experience.[18]

A new kind of doctor-patient relationship needs to emerge to take advantage of the information and technology savvy consumer.

[15] eMarketer, September 2012.

[16] Mobil-ology, Ipsos Reid, January 2013.

[17] Ibid.

[18] Source: http://www.canhealth.com/tfdnews0663.html

Consumers have embraced the new capabilities that the mobility movement has created. Consider that there are more than 40,000 mobile health apps and hundreds of devices that allow consumers to track vital signs and wellness indicators in real time. Worldwide, consumers downloaded 24 million health apps in 2012, more than double the number from the previous year.[19]

However, this explosive growth isn't without its own management related challenges for clinicians who want to use mobile devices and mobile apps for professional purposes. Clinicians may have to sort through thousands of available mHealth apps that target them as an end user. As such, there may be a need for HDOs and providers to rely on the certification and curation of medical devices and mobile apps. There may be a need to validate the quality of an app's interoperability, privacy, security and content features to ensure patient safety. Clinicians will want these assurances before they begin to use mobile apps in a professional capacity.

[19] Source: http://www.alliedhealthworld.com/visuals/smartphone-healthcare.html

6. Value Proposition for the Use of Mobile Devices and Apps in Health Care

The use of mobile devices is an important enabler that *Infoway* believes can address several of the key challenges facing health care systems, such as the need for greater cost and process efficiencies and for the delivery of care in lower cost settings. For example, functions that were not possible without the mobile platform are now available for deployment and include real-time monitoring and alerts using wireless devices and sensors to inform clinicians on the status of their patients':

- diagnostics and health states
- behaviours, activities and medication compliance.

Many functions that can be performed using PC based clinical information systems are being ported to mobile platforms. This means that on-the-move clinicians have new channels and flexibility to complete routine tasks such as:

- communicating with colleagues
- accessing patient medical records including diagnostic and radiological images
- consulting reference sources such as drug formularies and dosing guidelines, clinical practice guidelines and HDO policies
- ordering tests and procedures (e.g., CPOE)
- clinical documentation.

Infoway believes that mHealth will increasingly play an enabling role in shaping new models of care.

The growth in patient self-management and patient engagement is well suited for mHealth technologies. Mobile devices and apps provide the tools for patients and informal caregivers to collaborate more effectively with their clinicians. A recent study concluded that patients who used digital health technologies felt better prepared for clinical encounters and asked more questions that were relevant to their condition.[20] However, more than new mHealth technologies are needed to support the provider and patient relationship. It requires new work processes to support the provision of health services and interactions with patients. It also impacts the way in which clinicians interact with one another and their digital health ecosystem.

[20] Pew Internet & American Life Project. (2012). From http://pewinternet.org/

7. Examples of the Use of Mobile Devices and Apps in Health Care

On-the-go clinicians use their mobile device to confer with colleagues, query drug and medical references and expedite orders to optimize patient throughput. While there are many applications for the use of mobile devices in health by clinicians, some of the more common use cases involving patients include:

- remote access to patient information
- texting to promote health
- improved transitions of care
- remote patient monitoring.

7.1 Remote Access to Patient Information

Mobility has ushered in new demands and expectations on the health enterprise from all classes of users, including clinicians, who are leading the mobility movement particularly surrounding access to medical knowledge and peer communications. However, their ideal is to use mobile devices to extend the reach of the electronic health record. According to a 2011 study completed by QuantiaMD Research, access to EMR data tops the wish list for how physicians want to use mobile technology.[21]

The Ottawa Hospital

The Ottawa Hospital's clinicians have been pioneers in use of mobile devices to transform health care delivery. In November 2010, the hospital began a small pilot project involving about 20 internal medicine physicians who used Apple's iPad tablet to remotely access the hospital's electronic health records repository. The clinicians quickly recognized the value of the tablet to their workflow. They were no longer required to be tethered to an office or ward workstation to access patient information. Instead, the tablet enabled anywhere and anytime access which meant their treatment decisions were better informed and made in less time.

Based on the overwhelming success of the pilot, The Ottawa Hospital supplied approximately 2,000 iPad2 units to its physicians, residents, pharmacists and many other professional staff. The hospital also developed an in-house app called the Clinical Mobile Application to provide physicians with access to information resources (e.g., drug formulary and medical journals) as well as the ability to view lab results, diagnostic imaging reports and transcribed documents. It continued to enhance the

[21] Tablets Set to Change Medical Practice, QuantiaMD Research, June 2011.

app with a picture archiving and communication system (PACS) viewer and voice recognition recording for electronic physician orders and notes. Clinicians are also able to connect with the hospital's regional and provincial EHR ecosystem from their tablets. They can view orders and results such as the X-rays, CT scans and lab tests in the province's EHR repositories.

The iPad and the Clinical Mobile App have enabled physicians to significantly reduce the time they spend reviewing patients' cases before making their rounds each morning. By eliminating lengthy meetings to review each patient's case as well as the time needed to travel between patient rooms and stationary PCs, the hospital estimates that its physicians save approximately two hours per day in their clinical care activities. The iPad has also increased engagement between providers and patients as bedside rounds have become common practice again, replacing conference room based daily rounds. Doctors also found that the iPad assisted with communicating test results to their patients and with teaching them to better understand their conditions and treatment plans.

The Ottawa Hospital estimates that the iPad and Clinical Mobile App has saved its physicians approximately two hours each day.

Infoway asserts that every future software solution deployment which supports clinicians should consider including a mobile user interface option to multiple platforms, as exists at The Ottawa Hospital. Apps should form part of an interoperable digital health ecosystem to deliver the full functionality, convenience and value that clinicians want from their electronic interactions with the health care system.

7.2 Texting to Promote Health

Cellular phones have become so widely available that it is believed more people use them than tooth brushes.[22] Further, it is predicted that "nearly four billion smartphones will be sold between 2011 and 2015 giving users access to all of humanity's collective knowledge in the palm of their hand."[23]

Developing and developed economies have taken advantage of the mobile phone penetration to reach underserved populations with health services. Simple functions can reap big benefits. As an example, in many African countries where there is an absence of health information and communication technology (ICT) infrastructure, texting is used to support infectious disease surveillance activities, order supplies and meet the communication needs among health professionals. It has resulted in

[22] Paul Jacobs, PhD, Chairman and CEO of Qualcomm. Keynote address to the mHealth Summit 2011, Washington, DC. December 12, 2011.

[23] Ibid.

expedited processes to log the diagnosis of communicable diseases leading to earlier detection of outbreaks, improved timeliness of communication and management related to outbreaks, and improved procurement logistics for ordering of medications and supplies to combat the outbreaks.[24]

In developed economies short message service (SMS) texts are used to support patient behavioural changes through education, motivational messages and reminders. Texting based interventions have been deployed for smoking cessation, chronic disease and maternal and child health programs. Clinicians should be aware that there are automated means which may already be part of their existing practice solutions or available in other software (e.g., chronic disease management tools) that could be used to support that capability.

7.3 Improved Transitions of Care

Hospital readmissions are all too common, yet many of these costly events can be avoided.[25] More than one third of Ontario patients discharged from internal medicine wards are readmitted to hospital within 90 days.[26] This is believed to be attributable to service and coordination gaps between primary care, acute care and home care programs. In Ontario, the cost of readmissions has been estimated at more than $700 million per year.[27]

In recent years, a new model of care known as virtual wards has been adopted by some hospitals to reduce the rate of readmissions. These new programs, staffed by interdisciplinary teams from primary and community care organizations, provide short term transitional care to high risk patients who have recently been discharged from hospital.[28]

mHealth device solutions can also play a vital role to improve continuity and transitions of care which are important goals of health systems everywhere. In the same context, mHealth can be used to engage and empower patients through self-management of their conditions.

---

[24] *Racing a Disease*; Fast Company Magazine, October 2012.

[25] CMAJ. 2010 April 6;182(6):551-7. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2845681/

[26] CARP; 2011. [cited 2011 Aug 17]. Available: http://www.carp.ca/advocacy/adv-article-display.cfm?documentID=6061

[27] Ibid.

[28] LHINfo Minute Health Care Update. Available: http://www.torontocentrallhin.on.ca/uploadedFiles/Home_Page/News_Rooms/LHINfo%20Minute%20-%20Virtual%20Ward.pdf

In 2011-2012, Women's College Hospital (WCH) in Toronto, Ontario piloted the use of a cloud-based mobile solution to enhance the quality of recovery and to ensure patients were safely discharged after a surgical procedure. Patients enrolled in the study used mobile phones for 30 days after their discharge from hospital. Using a mobile app, they completed a quality of recovery questionnaire and also took daily images of their surgical incision using the camera function on the mobile phone. The WCH surgeons used tablets to view the patient results and were able to reliably assess the quality of recovery. The mobile devices enabled the surgeons to identify developing complications such as post-operative infections and to share educational materials with their patients. And most importantly for an ambulatory centre, the WCH surgeons were able to achieve an average post-operative length of stay of 18 hours for a TRAM flap (breast) reconstruction patient compared to an industry average of 6.4 days.[29] Other results included cost savings from supporting patients at home after a shorter hospital stay, early interventions to treat complications, reduced readmissions and emergency department visits, and lower surgeon billings. Patients reported higher levels of satisfaction, reduced travel to medical appointments and reductions in wait times to access their care team.

Women's College Hospital surgeons were able to effectively and remotely manage the recovery of post-operative patients who underwent breast reconstruction. Inpatients were discharged on average 18 hours post procedure vs. an industry mean of 6.4 days.

7.4 Remote Patient Monitoring

With aging populations, chronic disease management has emerged as the greatest challenge for resource strained health systems in developed economies. The majority of primary care visits and admissions to hospital emergency departments are related to chronic diseases.

Mobile devices, apps and monitoring sensors are enabling tools for clinicians and patients to manage chronic illnesses outside of the hospital setting. Such devices transcend geographic boundaries and extend the clinician's service reach into the patient's home. Health measures can be captured automatically by devices (or manually by patients) and electronically transmitted back to the care team. Software algorithms can assist in assessing the patient data and alerting care providers to the

[29] Source: John Semple MD, Surgeon in Chief Women's College Hospital, University of Toronto presentation to 9th Annual Mobile Healthcare Summit, Toronto, Canada. January 31, 2013. For reference on the TRAM flap procedure: http://en.wikipedia.org/wiki/TRAM_flap

need for intervention. Early response actions may prevent a secondary care setting episode and lead to better health outcomes for the patient.

Remote patient monitoring technologies that deliver information directly to clinicians have also been applied in hospital settings to improve peer communications and reduce patient risk. For example, the Federal Drug Administration (FDA) approved AirStrip OB™ has been used by U.S. hospitals to deliver live patient waveform data (e.g., fetal heartbeat and maternal contraction patterns) directly from the labour and delivery unit to the clinician's tablet or smartphone. Busy clinicians can remotely monitor their patients when the demands of their role require them to attend to tasks in other locations, resulting in a fourfold increase in clinician utilization.[30]

It is increasingly common for HIS and EMR vendors to offer mobile apps that enable clinicians to monitor their patients. Other mobile apps are available to assist with remote care delivery including those that allow health care practitioners to perform real time medical consultations from anywhere using a smartphone. Additionally, apps such as Wellx™ enable physicians and their patients to securely message one another, share results and send reminders.

Juniper Research predicts that by 2016 the number of patients monitored over mobile networks will reach three million globally. The firm believes that increasing smartphone processing power along with new health care peripherals will result in increasingly more clinicians partnering with their patients to use the smartphone as a home health hub. Juniper further asserts that the shift will also lower the cost of remote patient monitoring since it will reduce the need for costly dedicated health devices.[31]

[30] Source: Claim has been published in AirStrip OB™ marketing materials by AirStrip Technologies.

[31] Source: Juniper Research press release. February 2, 2012.

8. The Benefits and Economics of Mobile Computing in Health

8.1 Hype versus Evidence

As typical of new technologies, there has been a lot of hype and promise surrounding the capabilities and benefits of the use of mobile devices in health care delivery. In contrast to the predictions of improved efficiencies, effectiveness and cost reductions, the available outcome results from evaluation studies have been mixed.

This may be explained in part by the rapid pace of technological advancement versus the markedly slower pace of research. Randomized control trials (RCTs) are often seen as the gold standard to test the effectiveness of medical interventions. But it can take up to several years for RCT studies to be published. Results may be of limited relevance to HDOs and clinicians should the evaluated technology already be obsolete by the time the research is published.

8.2 What Does the Research Say?

In a word: mixed.

A systemic review of more than 60 studies concluded that text messaging health care interventions used by providers were for the most part clinically beneficial, in public health related uses, and in terms of administrative processes. However, despite the promise of these findings, the researchers observed that literature gaps exist, especially in primary care settings, across geographic regions and with vulnerable populations.[32]

In another systemic review, British researchers examined 70 studies conducted over 20 years on mobile interventions delivered to health care consumers and mHealth technologies intended to improve care delivery processes. They found modest clinical benefits (e.g., smoking cessation). However, most behavioural interventions were not successful. Administrative functions such as appointment reminders were effective.[33]

Other primary research studies have demonstrated the efficacy of mobile devices in the management of chronic disease patients. Logan et al demonstrated that a home blood pressure telemonitoring system, which provided self-care messages on the smartphone

---

[32] Valerie A. Yeager, Nir Menachemi (2011), Text Messaging in Health Care: A Systematic Review of Impact Studies, in John D. Blair, Myron D. Fottler (ed.) *Biennial Review of Health Care Management (Advances in Health Care Management, Volume 11)*, Emerald Group Publishing Limited, pp.235-261.

[33] Free C, Phillips G, Watson L, Galli L, Felix L, et al. (2013) The Effectiveness of Mobile-Health Technologies to Improve Health Care Service Delivery Processes: A Systematic Review and Meta-Analysis. PLoS Med 10(1): e1001363. doi:10.1371/journal.pmed.1001363

of hypertensive, diabetic patients immediately after each reading, improved blood pressure control.[34] Seto et al research provides evidence of improved quality of life through improved self-care and clinical management from a mobile phone based telemonitoring system. The use of the mobile phone based system had high adherence and was feasible for patients, including the elderly and those with no experience with mobile phones.[35]

Park and Kim investigated the effects of a combined mobile phone and computer messaging intervention in reducing waist circumference, blood pressure and lipids in obese, post-menopausal Korean women. After 12 weeks, these women were found to have significant reductions in waist circumference, blood pressure and LDL cholesterol in comparison to the control group participants who experienced increases in these same measures.[36]

8.3 What are the Economic Impact Predictions?

While many industry analysts believe that mHealth can result in significant economic savings, improved efficiencies and quality of care, there are mixed results between forecasts and evaluation studies. For example, a recent study completed by Boston Consulting Group (BCG) and Telenor Group predicted that mobile health projects in developing economies could:

- help physicians reach about twice as many rural patients
- improve tuberculosis treatment compliance by between 30 per cent and 70 per cent
- reduce elder care costs by about 25 per cent
- reduce maternal and perinatal mortality rates by about 30 per cent
- reduce medical data collection related costs by about 24 per cent.[37]

[34] Logan AG, Irvine MJ, McIsaac WJ, Tisler A, Rossos PG, Easty A, Feig DS, Cafazzo J.A. Effect of Home Blood Pressure Telemonitoring With Self-Care Support on Uncontrolled Systolic Hypertension in Diabetics. Hypertension. 2012 Jul;60(1):51-7.

[35] Seto, E., Leonard, K. J., Cafazzo, J.A., Masino, C., Barnsley, J., & Ross, H. J. (2012). Mobile Phone-Based Telemonitoring for Heart Failure Management: A Randomized Controlled Trial. Journal of Medical Internet Research. 2012 (Feb 16); 14(1):e31.

[36] Park MJ, Kim HS. Evaluation of mobile phone and Internet intervention on waist circumference and blood pressure in post-menopausal women with abdominal obesity. International Journal of Medical Informatics. doi: 10.1016/j.ijmedinf.2011.12.011.

[37] The Socio-Economic Impact of Mobile Health, Boston Consulting Group/Telenor Group, April 2012.

A 2012 study of the U.S. wireless industry found mobile devices improve worker productivity by:

- reducing unproductive travel time
- improving logistics
- enabling faster decision making
- empowering small businesses and improving communications.[38]

It is estimated that industry realized increased productivity valued at $33 billion in 2011 alone. One third of this estimate ($11.2 billion) was attributed to the medical sector. Further, there were projected productivity gains of $305.1 billion over the next 10 years in medicine.[39]

A recent report (2012) by Deloitte's Center for Health Solutions projects that telehealth tools, home health monitoring devices, smartphones and tablets, and videoconferencing will serve to expand the reach of physicians. Deloitte forecasts that commonly available teleconferencing tools like Skype™ will allow for remote consults between physicians and patients resulting in:

- 24 per cent fewer hospital admissions and
- a 26 per cent decrease in the average length of inpatient stay.

Similar to the BCG/Telenor study, Deloitte believes that remote monitoring tools will free up resources to reduce the cost of caring for rural patients. In the case of elderly patients, the immediate savings could be as much as one quarter of the present cost with additional savings of $200 billion over 25 years. Deloitte's study also found that physician productivity increased with the use of mHealth applications in the hospital setting. Approximately 63 per cent of physicians reported increased productivity, with a small minority (6 per cent) experiencing at least a 50 per cent increase in their efficiency.[40]

The cost of caring for elderly patients could decline by 25 per cent and save the U.S. health care system $200 billion.

[38] Roger Entner, "The Wireless Industry: The Essential Engine of U.S. Economic Growth", Recon Analytics, May, 2012, pp. 30-33 as cited in "mHealth in an mWorld: How mobile technology is transforming health care," Deloitte, 2012.

[39] Ibid.

[40] mHealth in an mWorld: How mobile technology is transforming health care, Deloitte, 2012.

A recent Canadian assessment (2012) of the economics of home telemonitoring for patients with various chronic diseases indicated significant benefits. Results included large reductions in the number of hospitalizations, average length of inpatient hospital stay and emergency room visits. While the number of home visits by nurses increased, the telehomecare program resulted in significant savings: the equivalent of more than $1,557 per patient on an annualized basis as compared to traditional home care.[41]

Conversely, a 2013 study in the United Kingdom by Henderson et al on the cost and cost effectiveness of telehealth (encompasses real time monitoring of vital signs) in addition to standard support and treatment for patients with long term conditions, concluded that telehealth solutions did not seem to be a cost effective addition to standard support and treatment.[42]

Infoway believes that mHealth holds promise for quality and efficiency improvements in many aspects of health care delivery. However, we encourage the industry to continue to undertake investigations on the cost and benefit of mHealth technologies to support future deployment decisions.

[41] Home Telemonitoring for Chronic Disease Management: An Economic Assessment, HEC Montreal, August 2012.

[42] Henderson, C. et al, Cost effectiveness of telehealth for patients with long term conditions (Whole Systems Demonstrator telehealth questionnaire study): nested economic evaluation in a pragmatic, cluster randomized controlled trial, BMJ 2013;346:f1035 doi: 10.1136/bmj.f1035 (Published 22 March 2013).

9. Business Considerations for the Use of Mobile Devices and Apps in Health Care

There is much to be considered by any HDO executive or IT strategist leading the deployment of mobile solutions in their health delivery organization. The goal of this section is to present some of the key considerations organized by their business impact.

The following key assertions are presented:

- consumerism is driving clinician use of mobile devices
- clinicians consume and generate information and services
- HDOs must plan and manage their mHealth initiatives in a strategic or proactive approach
- the use of mobile devices in health care delivery represents new and significant costs for the organization.

9.1 Consumerism as a Driver for Clinicians

Clinicians use their smart devices for professional purposes even in the absence of formal mobile solutions

Clinicians routinely experience the expanding capabilities of smart devices and apps in their private lives. There is the expectation about convenience and efficiency of anywhere, anytime, any device computing. Like all mobile device consumers, they have embraced the self-empowering opportunities that their Internet connected devices have made available to them. Often clinicians will evaluate, select, acquire and install professional medical apps on their smartphones and tablets without the guidance of an HDO policy, quality assurance and assistance of their enterprise's IT resources.

Considerations for clinicians, patients and Health Delivery Organizations

A quickly shifting environment in which clinicians and mobile computing coexists is threatening traditional centrally planned and executed IT business models. Clinicians and patients need to be made aware of the privacy and security implications of using mobile devices and apps for professional purposes. This issue is dealt with extensively in Section 11.

Where appropriate, organizations should make clinicians aware of, and agree with, where personal health information is held, how it may be used, and ideally have some transparent means of monitoring its access and use. The ease of acquisition of cloud based mobile health apps may hide or obscure this fact for the end user.

9.2 Clinicians are Consumers and Generators of Information

Clinicians expect to be able to use a spectrum of applications that are function specific and operate against a consistent backplane of comprehensive patient data

Clinicians are consumers and generators of information. For example, they create information when diagnostic tests are ordered and they consume information when viewing results.

Pervasive networking and mobile computing are causing clinicians to expect to be able to service their patients in different care settings and contexts. Clinicians will have high expectations for the responsiveness and high availability of mobile applications.

Considerations for Health Delivery Organizations

HDOs that want to deploy mobile technologies and applications need to plan and articulate investment priorities and ways forward in their enterprise information technology and services strategy. Clinician users should be engaged in the planning so there is a clear understanding of the context in which they'll use the mobile service. Greater discussion of the considerations of mobile computing and the enterprise IT strategy is provided in Section 10.4.

Consideration must be given to the reliability and regulatory status of any mobile app used for professional purposes. Also, as was discussed in *Infoway's* Cloud Computing in Health White Paper, HDOs need to be aware of the cloud based technology they employ for their mHealth solutions, their rights and obligations in its use, and what happens to data they collect using this technology (the data related to what they do, as well as the data of the patients they treat). Privacy and security issues similar to those raised in considerations for individuals are applicable to health care providers using cloud services.

Clinicians also need to consider that any cloud based technology and apps they acquire individually will require unique credentials and login. Unless information sharing is enabled by their organization or jurisdiction, the data they access and collect through that technology may be completely siloed and segregated from other relevant information they may need or expect, to fulfill their professional responsibilities as providers of health services.

9.3 Planning and Managing mHealth Initiatives in a Strategic or Proactive Approach

Many mobile expansions are fragmented with overlapping approaches to planning, procurement, governing policy, application design and end user support

Many mobility initiatives have been led by clinical champions and anchored in pilot projects, often at the edges of the health enterprise. Early successes have led to increased clinician demand, and in some cases, rapid expansion. What results is limited business alignment between centrally planned IT and the HDO's business units with the trade-off being sub-optimal efficiencies. More tactical than strategic, many mobile expansions are underscored with fragmented and possibly overlapping approaches to: governance, planning, procurement, security policies, cost (capital and operations), application design and end user support.

Considerations for Health Delivery Organizations

Infoway has observed that HDOs are reverting to a solution deployment approach that was quite common in Canada 10-20 years ago, namely custom development. This is justified in a rapidly changing technology environment, one that is disruptive and innovative, and somewhat nascent.

Many mobile expansions are fragmented with overlapping approaches to governance, planning, use, security and support.

The build or buy question is one that HDOs, health regions and even health ministries will have to wrestle with. While earlier adopters have trended toward solution build – in some cases out of necessity – *Infoway* recommends an approach that leads to more commercial off-the-shelf (COTS) solutions and open source systems (OSS) which have similar advantages. We are beginning to see that HDOs, even the largest, such as Kaiser Permanente and Partners Healthcare (Boston, MA) are moving away from custom development to COTS for their EMR/EHR solutions. These organizations have realized that they are not experts at software development, but rather their core expertise is in delivering care. And, they cannot amortize the cost of solution development like a vendor can over a much larger market and install base.

Many HDOs will attempt to address the issues of fragmented approaches by developing a separate mobility strategy to drive their expansion. However, the mobile strategy should not be a free standing document. It needs to form part of a broader set of business and technical strategies and corporate policies.

Here is Gartner's recommendation: "A *revised IT strategy that incorporates and is influenced by mobility is the best objective. To maximize the value of mobility, IT must lead the entire organization through a comprehensive review of how it will invest in and use mobility to support business performance objectives. The results should be used to improve current IT and business practices, rather than to call out mobility as a uniquely different practice."*[43]

Infoway is in agreement with this recommendation. An HDO's mobility strategy needs to be thought through in context with its other digital health investments such as HIS, EMR, EHR and health analytics.

9.4 Mobile Devices Represent New and Significant Costs for the Health Delivery Organization

Bring Your Own Device model is a strategy which may serve to mitigate the financial impact of going mobile

The use of mobile devices in health care delivery will require capital and ongoing operating investments. These expenses represent new and significant costs for the organization, and as such, are a major barrier for many HDOs. Consider a scenario where a hospital is switching from pagers to smartphones. Monthly wireless plan fees could increase markedly, from approximately $5 to $80 (or more), for each user.

The Bring Your Own Device (BYOD) model can mitigate the financial impact of going mobile. Business unit leaders, their employees and physicians need to carefully consider the possible cost sharing arrangements for mobile device use.

Considerations for Health Delivery Organizations

The mobile environment is evolving rapidly with new devices, features and functionalities regularly entering the market. The BYOD model is potentially more responsive to changing business needs and consumer choice and has gained traction within many HDOs.

In a BYOD arrangement, the HDO is likely able to entirely avoid or substantially mitigate the capital cost associated with acquiring smart devices for its staff (which could number into the thousands of units) by requiring them to supply their own device at their expense or by sharing the cost in recognition that it will be used for personal as well as professional purposes. An advantage of the BYOD model is that little device training may be required as experienced users are already present within the organization.

[43] Gartner report G00201262 "Put an Integrated Mobile Strategy in Place, or Face Increased Costs Later."

A second cost consideration is the operating expense of smart devices. As employees and physicians will use their devices to conduct business on behalf of the HDO (while on the go and out of range of the HDO's Wi-Fi network), it is reasonable to assume that some portion of the user's voice and data costs will be expensed back to the business unit. In recognition of the dual purpose and use of the devices, the HDO may wish to establish a cost sharing arrangement with the users to plan for operating budgets.

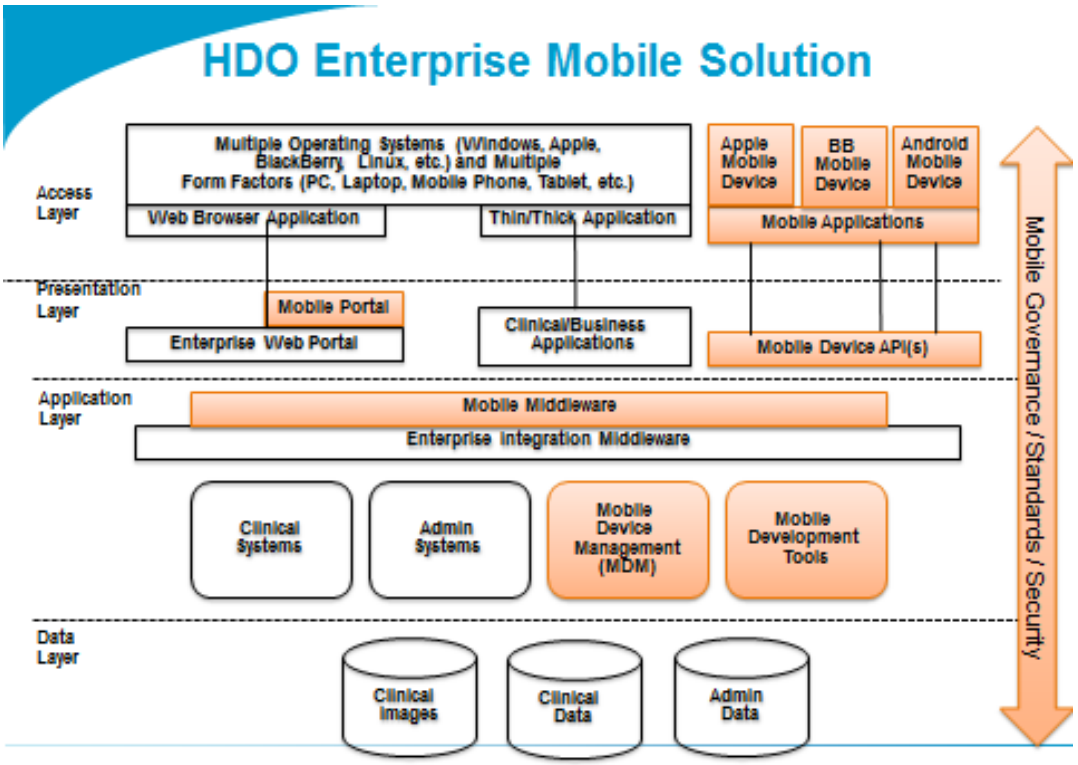
While there are many benefits to a BYOD environment, organizations must also consider potential increases in costs associated with the management of multiple devices and application platforms versus the enterprise owned model. To reduce the complexity and cost of managing multiple devices, systems and security integration, the HDO may want to exercise a degree of control by limiting the range of supported devices and platforms.

10. Enterprise Deployment Models

This section is primarily written for IT planners or strategists who make decisions affecting the HDO's mobile strategy and deployment. This section focuses on identifying the considerations for deploying mobile devices that are integrated with an HDO's enterprise information systems.

Figure1 depicts potential changes to an HDO's enterprise architecture to support mobile devices and applications.

Figure 1 – HDO Enterprise Mobile Solution



The orange boxes represent mobile functionality (e.g., managing mobile devices, developing mobile applications) that can be added to an existing architecture (the gray boxes). The orange boxes are further explained in the next sections.

The following key assertions are presented in the next sections:

- mobile middleware can facilitate the integration of mobile devices into the HDO's information systems
- to ensure a successful and sustainable mobile device deployment, HDOs will need to implement or upgrade mobile device management tools
- there are emerging mobile standards that could affect the data collected and exchanged between mobile devices and apps and HDO information systems

- mobile devices and applications should be included in the HDO's enterprise information technology strategy
- a successful mHealth deployment requires a governance framework. (See section 10.5 mHealth Governance for details.)

10.1 Seamless Integration

Mobile middleware can facilitate the integration of mobile devices into the HDO's information systems

Mobile middleware is defined as software used to connect disparate mobile applications, programs and systems. It essentially hides the complexities of working in mobile environments, allowing for smoother mobile computing integration and mobile app development[44]. Accessing enterprise data on mobile devices introduces complexities like "online" and "offline" requirements, support for multiple mobile devices, operating systems and the use of mobile protocols optimized for low bandwidth networks (cellular networks).

Many HDOs use middleware today to streamline access to multiple enterprise data sources. The value proposition for traditional enterprise middleware is largely based on reducing the complexities and costs of maintaining interfaces to more than three enterprise data sources [The N(N-1) rule]. Gartner Research has extended this concept to the "*Rule of Three*" for mobile environments. When the enterprise requires:

- support for three or more mobile applications
- support for three or more mobile operating systems (OS)
- integration with at least three back-end data sources.

"Rule of Three"

The use of mobile middleware becomes viable when an HDO requires:

- *support for three or more mobile applications*
- *support for three or more mobile operating systems*
- *integration with at least three back-end data sources.*

The costs and options for building, supporting and maintaining mobile apps, mobile operating systems and interfaces to data sources within an enterprise become challenging to sustain. The introduction of mobile middleware, mobile development and management tools can simplify the sustainability of the HDO's mobile environment.

Mobile middleware can speed application development and increase consistency across mobile applications and mobile platforms via support for multiple mobile client application programming interfaces (APIs). Traditional applications assume the end

[44] SearchSOA - http://searchsoa.techtarget.com/definition/mobile-middleware.

user is accessing the application from a fixed workstation with unlimited power and bandwidth. This is obviously not the case with mobile access. Mobile middleware helps alleviate this problem through the use of caching and buffering.[45]

In addition, mobile middleware supports the same functionality as traditional middleware with the additional support for specific mobile platforms, standards and functionality, like data synchronization, security and optimization from back-end system to the mobile device.

Considerations for Integrating Mobile Apps

HDOs have a couple of options when providing mobile access to internal information systems *(as a general guiding principle remember the "Rule of Three" when considering the following two bullets):*

- Address each back-end system independently, purchasing or building apps as required for each of the supported mobile devices.

  or

- Adopt a mobile middleware approach that adds a layer of abstraction to the back-end system integration, and provides tools and functionality for supporting multiple mobile client operating systems.

There are foundational components in existing middleware platforms used by HDOs today that should be re used when providing data access to mobile devices and apps. These include, but are not limited to, support for multiple interface standards, creating a level of abstraction, and enforcement of security policies and services. Ideally, adding mobile middleware capabilities to existing platforms and services will increase consistent access across traditional fixed workstations and mobile devices.

10.2 Mobile Device Management

To ensure a successful and sustainable mobile device deployment, HDOs will need to implement or upgrade mobile device management tools

Organizations planning to deploy and manage mobile devices are faced with several challenges. Those challenges include, but are not limited to: the need for mobile use policies, configuration, deployment, application licensing, and mobile device and app support. The challenges can deepen once decisions are made for:

- The number of device platforms supported within the organization (e.g., Blackberry, Apple, Android, Windows).
- Use of organization owned mobile devices and apps versus employee owned mobile devices and public apps (i.e., BYOD).

[45] Dept. of Computer Science – University College London – Principles of Mobile Computing Middleware.

There are requirements for supporting functionality that are specific to the challenges of managing mobile devices. Some examples include device discovery and enrollment, app management and distribution, performance monitoring, security features (e.g., remote wipe) and policy management.

Considerations for Mobile Device Management

- HDOs should evaluate their mobile device management (MDM) requirements against available vendor mobile device management solutions. Features such as supporting remote management, device inventory and policy enforcement are common among multiple MDM vendors for a single mobile operating system. However, if you require the same features across multiple mobile operating systems the number of vendors decreases significantly. A good resource tool for comparing the features of competing products is the MDM Comparison Tool[46]. As of June 2013 there are 44 MDM vendors registered. HDOs that require a MDM vendor to support the three popular operating systems – iOS, Android and Blackberry, plus some basic integration into lightweight directory access protocol (LDAP) for authorization and authentication – will find that 15 out of the 44 products can meet their requirement. Depending on the HDO's mobile strategy for supporting multiple mobile operating systems and the features required to integrate into the overall HDO technology infrastructure, the choices can be presented quickly using this tool.

- A BYOD support model will result in the need for specific qualities in an MDM. For example, advanced features like the ability to separate personal and corporate profiles, the ability to block access to certain device capabilities (e.g., device camera), and control over apps that could compromise an HDO's network.

- There are costs associated with owning and operating the MDM platform. This includes the obvious costs of software, and hardware, but also the resourcing costs to operate and support the MDM platform and mobile users. There is limited research available specifying human resourcing costs associated with MDM. One research paper points to the need for additional IT staff when managing and supporting an "in-house" MDM solution.[47]

- An outsourced MDM solution might be a consideration for HDOs looking to minimize their IT capital costs and resource requirements and still provide the services of MDM.

---

[46] EnterpriseIOS – MDM Comparison Tool - http://enterpriseios.com/wiki/Comparison_MDM_Providers.

[47] Mobile Devices in the Enterprise, Osterman Research White Paper, July 2012.

10.3 Emerging Mobile Standards

There are emerging mobile standards that could affect the data collected and exchanged between mobile devices and apps and HDO information systems

The "mHIMSS Roadmap" lists 17 standards and mobile interoperability organizations that are involved with mHealth standards.[48] Many of these are familiar participants in the health care standards arena, like Continua, IEEE, ISO and HL7. The categories can be further divided by mobile device, application and interoperability standards. This section focuses on the interoperability standards category as it relates to HDOs.

Mobile device and app interoperability standards play an important role for an HDO that is integrating mobile devices with health information systems. A couple of relevant factors for the HDO are:

- Mobile devices and apps are becoming prevalent in health care, but are only just being recognized by traditional health care standards organizations (e.g., HL7)[49].
- Mobile device and app integration is rapidly evolving and largely non-standardized.

In addition to the prevalence of mobile apps in health systems, there's an increasing amount of health care data being captured by mobile devices and exchanged with HDO health information systems. In some cases the data is using the device as a conduit and the data is originating from sources like sensors and other wireless medical devices. This is further driving the need for standardization across devices and platforms.

These factors can easily lead to incompatibilities when sharing data between mobile devices platforms, and when exchanging data with health information systems.

Considerations for Mobile Standards

The application of mobile standards should be considered in the context of the HDO enterprise architecture (as per Figure 1). For example, the use of mobile middleware creates the need for mobile standards awareness between the middleware and the mobile device. The middleware removes the need for mobile standards awareness between the mobile device and the back end or external sources. (Assuming all data sources integrate with the middleware.) With this in mind there are a couple of standards considerations:

[48] mHIMSSRoadmap - http://www.mhimss.org/roadmap.

[49] Ibid.

- The number of available mobile standards and the need to seamlessly exchange data with other HDOs adds to the business drivers for the use of mobile middleware. Additionally, mobile middleware removes a layer of complexity for the mobile application developers by allowing them to focus on content and the presentation of the app and not the back-end integration.
- Organizations like the Continua Health Alliance and Open Mobile Alliance (OMA) are packaging the existing and emerging mobile standards into useable specifications and APIs that can be tested and certified. This can be a valuable starting point for HDOs who are new to the mobile standards arena.

10.4 Mobile in Enterprise IT Strategy

Mobile devices and applications should be included in the HDO's enterprise information technology strategy

From a technology perspective there are a number of factors contributing to the need for a mobile strategy:

- The HDO's ability to deploy and support mobile applications includes purchasing or developing, integrating and supporting mobile applications on one or more mobile device operating systems. To further drive the need for mobile strategy in this category, many of the common COTS health applications are offering a mobile option. In an HDO with multiple clinical systems offering mobile options, information silos, solution management and support inconsistencies could easily occur. This further emphasizes the need for a mobile strategy within the enterprise IT strategy to provide guidance and consistency between mobile applications and devices used within the HDO.

- HDOs are faced with increasing user demands to support mobile devices used by employees outside of work. These include devices that come in various form factors such as smartphones and tablets, and run different operating systems such as Apple, Android, Blackberry and Windows. In a mobile enabled workplace, HDOs will need to support business and clinical applications for traditional "fixed" workstations and provide the same or increased functionality for those users on mobile devices. The resources and tools needed to support mobile applications for each mobile operating system are different than the traditional requirements of supporting single operating systems (i.e., Microsoft Windows) with "fixed" workstation configurations.

- HDOs need to ensure technology tools are available to support and maintain a sustainable mobile environment. As stated in other sections of this document, there are unique requirements for managing and supporting mobile devices (i.e., MDM), building mobile focused applications (e.g., mobile development tools for Apple, Android, Windows and the Web), and integrating and presenting data between multiple systems and mobile applications (e.g., Mobile Middleware).

Without a comprehensive roadmap the HDO could experience an increased set of risks ranging from: IT resourcing and support, technology capabilities and cost, data and use governance, and enterprise privacy and security of corporate and personal health information.

Considerations for Mobile in the Enterprise IT Strategy

- Selecting a browser based or mobile app based approach will have influence on the development tools, sustainability and resources required. There are three application deployment approaches to use when providing user access to mobile content:
    - Provide users access to a mobile enabled website – this is a website that is accessed on the web browser included on the mobile device (e.g., Apple uses the Safari web browser). A mobile website can be optimized for smaller screens, and lower bandwidth connections.
    - Provide users access to mobile applications – these are applications requiring installation on the mobile device. The applications could support device specific features like camera, location, positioning, touch screen, as well as "off-line" and "on-line" connectivity.
    - Provide users access to both.

  (Note: standards such as HTML5 are used to create websites that look and function in a similar way to mobile applications, so the differentiation between the two approaches is becoming less distinct.)

- Determining which mobile operating systems to support or whether to support multiple mobile operating systems. This will affect the functional requirements of mobile tools and skill sets needed to support them.

- Deciding if the HDO should own or outsource its mobile technology (e.g., applications, development tools, management tools). The choices will affect the resourcing and financing of technology purchases.

- Determining what legacy technology can be repurposed for mobile by evaluating existing development, management and integration tools. This assessment will inform the roadmap approach to mobile device and application deployment.

- Understanding the requirements needed for an HDO to consider using a mobile module included with its current and future COTS health applications. This would take into consideration factors such as which mobile device platforms are supported, and mobile security and encryption. A COTS health application mobile module should be consistent with the existing enterprise IT strategy and not create inconsistencies for deployment, support and management.

10.5 mHealth Governance

A successful mHealth deployment requires a governance framework

Mobility's reach within the HDO is virtually limitless and can involve all employees from the executive suite to the support department. As previously noted, it is not uncommon for wireless communication mHealth initiatives to enter the HDO in many different ways across its business units.

The concept of consumerization of mobile devices and their apps has created the expectation of end user self-service empowerment. The easy and low cost of acquisition of medical apps on employee owned devices in a BYOD context will create mobile deployment governance challenges. Deployment of mobile devices without an overarching governance framework will result in confusion with regard to roles, responsibilities and accountabilities among users of mHealth apps and for HDOs that assume data custodial responsibilities. mHealth governance defines the people, processes and policies used to manage mobile devices and apps.

Deployment of mobile devices without the benefit of an overarching governance framework will result in confusion with regard to roles, responsibilities and accountabilities.

Considerations for mHealth Governance

- HDOs deploying mobile devices should implement a governance framework that defines how mobile apps and devices will be managed. This type of governance should address the function of mobile devices within an HDO's broader enterprise governance structure. Mobile device governance must be aligned with other governance processes within an HDO such as:
    - information strategies
    - risk management
    - IT governance
    - mobile app deployment model strategies.

- Mobile device governance should be considered as part of an overall IT and information governance process. A mobile governance process will facilitate a controlled yet responsive use and deployment of mobile devices and apps. An appropriate governance process will also help manage risks assumed by data custodians, thereby allowing for the protection of personal health information (PHI) as an asset.

- The governance process should include participation by clinicians in addition to IT managers and planners. The roles, responsibilities and accountabilities of the HDO's data custodians and clinicians should be clearly defined and articulated within policy and user agreements.

- A mobile device governance framework should include a mix of process and policy instruments. The following is a high level, non-exhaustive list of potential topics which should be addressed by processes or policies:

    - A policy or approval process for the use of mobile devices and applications within the HDO should exist. The policy could specify things like:
        - expectations for device operating systems (if management and support limitations exist)
        - versions of mobile operating systems and application software supported
        - processes and procedures for registration and access to HDO MDM client (MDM application client).

    - Identify who (e.g., group, department, individual) will be responsible for privacy and security of mobile devices, applications and their integration into the HDO enterprise. In addition, policy should be created to specify the role users and owners play when managing privacy and security on mobile devices and applications used within the HDO.

    - If applicable, policies and procedures for the use and connection of devices and apps in a BYOD context should be part of the governance framework. Organizations are encouraged to consider leveraging several public resources dedicated to BYOD policies.[50]

[50] http://searchconsumerization.techtarget.com/guides/Mobile-device-policy-guide-How-BYOD-policies-help-IT-manage-devices.

- Identify roles, responsibilities, processes and policies to support certification requirements for mobile devices and applications within the HDO. Certification of mobile applications should consider the privacy, security and interoperability aspects of the mobile applications.

- The overall governance of mobile applications, whether developed in-house, acquired from third parties or purchased from public app stores, must be addressed in a governance framework similar to any IT application in an HDO.

- Acceptable use guidelines, authority to manage devices, mobile apps and cost sharing should also be considered within policies.

11. Mobile Device and App Privacy and Security Considerations

11.1 Introduction to Privacy and Security Considerations

While the privacy and security requirements for mobile devices are similar to traditional computing platforms, they do require a unique set of considerations. Therefore, the approach to securing and ensuring the privacy of PHI on these devices differs from other computing platforms. As an example, traditional computing devices require a management infrastructure, policies and support staff to manage operating system patches, software versions and security policies. Mobile devices have the same management requirements. However, they must have a dedicated infrastructure (i.e., MDM) to achieve comparable results. Adequate preparation and a deployment program including MDM is critical for secure and privacy protective mobile devices within an organization.

While mobile computing devices may pose some risks, the good news is that several health care specific initiatives have made great advances in assisting organizations in deploying secure and privacy enhanced mobile devices. One such initiative is the HIMSS Mobile Security Toolkit [51] which provides detailed guidance on specific controls. The mobile device industry has also made great progress in developing enterprise level privacy and security and device management tools to assist organizations in meeting their requirements. *Infoway* feels it is important to view these risks in the context of convergence and integration with HDO information systems, EHRs and cloud computing.

Several health care specific privacy and security initiatives have made great advances in assisting organizations in deploying mobile devices.

This section of the paper will identify generic mobile device privacy and security concerns. However, the primary focus will be on considerations specific to the integration of mobile devices to the HDO's clinical IT services (e.g., CPOE) and information systems.

[51] http://www.mhimss.org/resource/mhimss-mobile-privacy-security-toolkit.

11.2 Generic Privacy and Security Concerns

What are the top privacy and security concerns of mobile devices?

A SearchSecurity survey of 487 IT security professionals and IT managers performed in the second quarter of 2012 has revealed the top four enterprise mobile security concerns and solutions. They are:

1. Device loss and theft
2. Application privacy and security
3. Device data leakage
4. Malware attacks. [52]

Device Loss and Theft

Device loss is the number one concern identified in the study. The small form factor of these devices makes them strong candidates for misplacement on public transit, in taxis, restaurants and airports.

The primary concern associated with mobile device loss is the access to confidential information either stored on the device or accessed by the device. This may put an organization's data, such as account credentials, access to email or PHI at risk to the tech savvy individual now in possession of the device. Typical solutions range from securing access to the device with pass codes, ensuring robust authentication of users accessing data or systems via a mobile device, or encrypting sensitive information stored on the device. The continuous interconnectivity of mobile devices allows for new device loss control mechanisms to be applied by MDM platforms which can be used to "remote wipe" device content. Organizations allowing for a BYOD policy may have an additional challenge when mobile devices are lost, as remote wipe capabilities may not be supported by all devices.

Application Privacy and Security

Privacy and security within mobile device applications has become a major concern as malware and privacy invasive apps are commonplace. In addition, the consumerization of apps has fueled the development of apps that may not have privacy and security features.

[52] http://searchconsumerization.bitpipe.com/data/demandEngage.action?resId=1356717614_813.

Device Data Leakage

Device data leakage is the ability to extract confidential information from devices, whether from lost or stolen devices or malicious apps. As mobile devices are integrated into HDO information systems, corporate access privileges must be controlled. Organizations must determine which corporate information assets can be accessed or stored on mobile devices provided appropriate security controls are in place.

Malware Attacks

The threat of mobile malware is an increasing concern as highlighted in several studies, including the Juniper Networks 2011 Mobile Threats Report published in 2012.[53] It found a 155 per cent increase in mobile malware across all mobile platforms when compared to the previous year. The study also found that in the last seven months of 2011, malware targeting the Android platform rose 3,325 per cent to 13,302 samples.

Other concerns identified in the study are:

- 30 per cent of applications have the ability to obtain the device location without users' explicit consent
- 14.7 per cent of applications request permissions that could lead to the initiation of phone calls without user knowledge
- 6 per cent of applications requested the ability to look up all the accounts on the device, including email and social networking sites
- 4.8 per cent of applications were able to send an SMS message without users' consent.

11.3 Privacy and Security Considerations for Integrated Mobile Devices

Infoway recognizes the availability of substantive literature on addressing generic privacy and IT security risks for mobile devices. However, there is little guidance when integrating mobile devices to HDO information systems.

The following section will present key assertions that *Infoway* feels must be addressed in the context of integrated mobile devices.

Those key assertions are:

1. Wide spread mHealth adoption by clinicians requires a seamless security experience.

[53] http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf.

2. Mobile device users expect devices and mHealth apps to be trustworthy and to protect the confidentiality of PHI.
3. Device users want a BYOD capability that is privacy protective and secure.

Wide spread mHealth adoption by clinicians requires a seamless security experience

Mobile devices have evolved to become very sophisticated personal computing devices, rivaling the performance and capacity of PCs. As a result, they are facing similar challenges, namely how to identify and authenticate access to the device, device apps, and locally stored data. Today's mobile devices have segregated security and privacy features. Device users may have several identities: one for the device, another for personal apps and potentially several more to access data from HDO information systems, so they will need to maintain and manage several identities and authentication schemes. This may negatively affect the rate of use of mobile devices in health care organizations, in addition to introducing security vulnerabilities.

Organizations providing mobile access to already siloed security schemes in their internal systems may simply perpetuate an already exasperating user experience for those who have mobile devices. Having different credentials and passwords of varying lengths that differ for personal and organizational apps becomes a usability challenge for any device user.

Considerations for Privacy and Security

- Organizations should consider the use of a ubiquitous identity credential and authentication mechanism(s) for mobile devices and mHealth apps. The identity credentials would be used for access to HDO information systems, as well as mobile apps. A common or federated authentication technique across mobile or cloud based apps and systems will provide for an increased and uniform level of confidentiality. Consideration should be given to cloud based Software as a Service (SaaS) Identity Management capability available for the issuance and management of common or federated identity credentials. Federated credentialing can be device based or device independent.

- Harmonization or federation of device, mobile app and health care organization system authentication schemes is recommended.

- In a BYOD context where several device platforms are supported, consideration of ubiquitous identity credentials that are mobile platform independent is recommended.

Mobile device users expect devices and mHealth apps to be trustworthy and protect the privacy of personal health information

The trustworthiness of devices, their operating systems and apps is crucial to continued adoption, integration and access to systems in the health care organization. Enterprises must continually demonstrate and ensure that mobile devices and apps meet the organizational security requirements, standards and policies.

For several years security researchers have been warning about mobile apps that request too many privileges, enabling them to tap into various data sources on the device. Mobile devices are more susceptible to this concern as operating system constraints may not allow for the separation of regular and privileged user accounts. Additionally, enterprise security policies may not be in place to restrict end user provisioning of apps. Take for example, apps built with ties to advertising networks, which make contacts, browsing history and geo-location data extremely valuable to marketers. The desire to monetize mobile apps is normal, considering that consumers want free apps, and ad networks will pay developers to get certain data from mobile device users. This raises serious privacy and security concerns when BYOD devices are allowed to connect to an organization's network and health care systems. This connection may expose provider or patient information as well as appointment calendars.

Considerations for Privacy and Security

- For mobile devices to be considered trustworthy and privacy protective, the day-to-day management of security and privacy features and devices is required. Device users and organizations must have confidence that the device is operating only authorized software and vulnerabilities are managed on a regular basis. This level of assurance is typically achieved by the implementation of MDM infrastructures and associated enterprise wide security policies and procedures. An MDM solution would allow, among other things, for the management of malware protection and integrity and security of apps. An MDM infrastructure provides administrators with control and visibility over the influx of personally owned devices connecting to the corporate network. Additionally, it constrains the ability to download and execute only authorized apps. MDM solutions can also be used to lock down corporate owned mobile devices so that employees cannot install unauthorized apps or browse random websites which reduce available organizational bandwidth.

- Privacy by Design (PbD) principles should be incorporated into the development of mHealth solutions and apps. More details can be found at the Ontario Privacy Commissioner's web site.[54]

- Organizations must ensure mobile device apps are trustworthy. Consideration must be given to how apps are evaluated and/or certified. The creation of a third party privacy and security and interoperability certification process for vendor and institutional developed mobile apps would remove a due diligence burden from health care delivery organizations which may not have the expertise or resources to evaluate vendor products. It would also have the benefit of increasing the level of assurance and trust organizations place in protecting PHI accessed or stored in mobile devices.

In a BYOD context, employees own the devices used to create, access and store Personal Health Information.

- In the absence of a formal independent certification process, HDOs should require vendor developed mobile apps to demonstrate privacy protective and security features. Organizations should consider using a due diligence process to ensure apps meet established requirements. Particular attention should be paid to the permissions used by acquired or in-house developed mobile apps.

- As identified in the previous section, a mobile app architecture deployment strategy can guide organizations in choosing the best mobile app architectures. When assessing the mobile app deployment strategy, consideration should be given to the use of browser based apps when accessing an HDO's information systems. Browser based apps can potentially provide added privacy and security benefits such as:

    - The storage of PHI in server based applications rather than mobile devices would provide an increased level of privacy protection.

[54] http://privacybydesign.ca/content/uploads/2011/05/IAPP_Canada-PbD_and_Mobile_Computing.pdf.

- When browser based apps incorporate the use of an HDO's common Active Directory Service it is possible to use the same corporate end user electronic credentials and passwords as an HDO's information systems. This allows for the reuse of common credentials, authentication techniques and authorizations for clinical systems whether using a PC or a mobile device, known as Single Sign On. This approach allows for the possibility of using cloud based web applications.

- The privacy and security benefits of this mobile app architectural approach should be balanced against any potential business constraints, such as the inability to use device specific features (e.g., camera).

Device users want a BYOD capability that is privacy protective and secure

BYOD introduces a unique set of challenges and considerations for HDOs and their ICT managers. The fundamental concept that influences many of the considerations is that of separate ownership. Employee owned devices have a shared usage which increases the complexity associated with device management, IT security and privacy safeguards as well as personnel information and apps. Therefore, the biggest risks for BYOD environments are control and privacy. Deploying and enforcing security controls is typically more difficult on personal devices for two reasons.

First, ownership of the device establishes a control mentality from the owner's point of view. Second, restrictions on personal data or content, in general, are more difficult to implement from a BYOD policy standpoint as these devices do not belong to the organization. As an example, if organizational backups of mobile devices cannot segregate personal apps and data from organizational ones a complete backup of the device may be required. In this instance, it is critical that organizations ensure the privacy of the user's personal information, apps and data such as personal correspondence, music and other media.

Considerations for Privacy and Security

- Once organizations have completed an assessment of the trade-offs associated with supporting a BYOD environment, they should develop a BYOD strategy and implement the appropriate security and operational policies and enforcement mechanisms to manage personally owned devices connecting to their networks. An example would be for employees who have lost a personal device to contact the organization's help desk to perform a remote wipe of the device prior to contacting their network provider to revoke network access. BYOD policies should apply to a wide range of issues from device loss or theft, data custodianship, app management, device and data ownership and obligations.

- BYOD policies and procedures should consider deleting an individual's personal data and content if included in device backups or corporate archiving systems. This applies to employees leaving the organization or when mobile devices are reported lost or stolen. The consent of the employee should be obtained when backing up employee personal data and content.

- Organizations should ensure all devices, including BYOD devices, adhere to corporate security policies and standards. This includes requiring employees to change passwords or support corporate authentication schemes on their personally owned devices. Personal devices should be subject to the same security safeguards as company equipment.

- Organizations need to clearly define and enforce minimum BYOD security requirements for personal devices used for business activities.

As BYOD devices are known to be a major source of malware introduction to organizational networks, consideration must be given to the implementation of automated flagging of known malicious apps and valid operating systems. MDM infrastructures provide this capability by using app blacklisting techniques.

12. A Call to Action

Mobile technology is being introduced to the health sector with much promise. In spite of the lack of empirical evidence of its efficacy at scale, many organizations are embracing mobile health capabilities.

Infoway's view is that mHealth is more than an emerging set of technologies. We are confident that mHealth will do more than provide the convenience of mobile computing to busy clinicians. We encourage HDOs to continue to deploy the technology to enable strategic system transformations that address the sustainability issues facing the industry. This includes the important objective of collaborating with partners to use mobile technologies to provide care to patients in lower cost settings.

Infoway notes that clinicians are embracing mobility and in some organizations are champions, leading their colleagues on mHealth projects. *Infoway* is confident that mobile devices and apps will continue to evolve and become a valued and trusted clinical tool.

Infoway reminds HDOs that the future state objective is to seamlessly integrate multi-platform mobile devices across the health enterprise's information and software services assets into its digital health ecosystem.

The following sections introduce some action steps that HDOs may wish to consider.

12.1 mHealth Leadership

Expectations from many clinicians are running high for mHealth solutions. Many HDOs are playing catch up with their clinicians who have found ways to adopt mobile health into their professional lives rather than wait for corporate initiatives.

Health enterprise leaders have a unique opportunity and responsibility to put in place the enablers that will support collaboration with their clinicians and digital health ecosystem partners to advance the mobile agenda. These opportunities and responsibilities include:

High Priority/Near Term Objectives

- Appoint an executive sponsor and expand scope of IT governance to provide oversight for mobility, alignment with business goals, and integration into all parts of the enterprise.

- Develop a mobile strategy that it is integrated into the broader health ICT strategy roadmap.

    - The introduction of mobile requires more robust ICT strategic planning and more due diligence to ensure alignment with the business requirements.

    - Begin analysis of current hardware and software assets and their readiness to support future mobile requirements. Begin to address any gaps to ensure readiness.
    - A strategy must have an element of agility as this space is evolving rapidly, especially in the areas of apps and MDM.

- Create a set of policies, standards, legal and regulatory frameworks that direct and guide the management and secure use of mobile devices and apps by clinicians, staff and patients.

- Avoid fragmented approaches to mHealth planning, sourcing, application design and support by centralizing decision making. This decision making must include the end users (clinicians) and IT. Understand the mHealth strategies, timelines, solution architecture and standards of your COTS vendors and incorporate them into your decision making.

- Ensure that future software solution deployments which support clinicians include a mobile user interface option to multiple platforms.

- Support a culture of innovation. Pursue partnerships with innovators within and outside the health enterprise. Leverage knowledge assets and goodwill.

12.2 mHealth Collaboration

Medium Priority/Near to Mid-term Objectives

- Initiate collaboration among regional health service partners and jurisdictional digital health organizations regarding mHealth strategic planning. *Infoway* recommends driving toward mobile device access to regional and jurisdictional applications (e.g., EHR or shared data repositories) and other digital health assets.
    - IT and clinical business unit leaders should collaborate to define clinical and business requirements. They should continually assess potential mobility functions, their strategic importance and fit and decide what capabilities to build internally or outsource, just as they would for any other technology. They can collaborate on joint procurement of solutions, development of solutions, operations and maintenance.

- Adopt and adapt other HDOs' knowledge assets into your mobile strategy such as road maps, use cases, business cases, and benefits evaluation frameworks.

- Engage and participate with standards development organizations that are developing enablers to support the health industry's transition to mobile health.

12.3 mHealth Execution

Infoway strongly asserts that mobile devices need to be integrated into the fullness of the health enterprise's clinical information systems and its digital health ecosystem. However, we predict that it may take five or more years for HDOs to reach that future state. IT leaders will be challenged to meet end user expectations for agility, while steering the HDO toward a more centrally planned and executed set of strategic mobility investment projects.

High Priority/Near to Mid-term Objectives

- mHealth initiatives should flow from a multi-year roadmap and target key use cases or business problems such as mobile access to: viewing the electronic patient record, viewing medical images and wave forms, medical references, order entry, remote patient monitoring, appointment scheduling, corporate intranet and commonly used forms.

- As new care models are developed, consideration should be given to fully lever the potential of mHealth. Leaders should be challenged to envision how mobility can help create new patient centred processes and patient centred engagement opportunities. Chronic disease management and virtual wards are two prime examples where mobile technologies can enable transformations in health delivery and patient engagement.

Medium Priority/Mid to Longer Term Objectives

- Consideration should be given to outsourcing components and contracting managed services (e.g., SaaS for MDM). Irrespective of where the service is sited, the goal should be to provide consistent policies and services across the device categories in use.

- Consideration should be given to the use of third party certification services for medical devices and mobile apps to assist clinicians in judging the reliability of an app's interoperability, privacy, security and content features to ensure patient safety. Clinicians will want these assurances before they begin to use mobile apps in a professional capacity.

- Consideration should be given to the use of third party (or in-house) curation services for medical devices and mobile apps to assist clinicians in finding and prescribing these solutions to their patients.

- Invest in mHealth training to meet skill requirements for IT staff and end users. Self-help education materials for clinicians should be available via the mobile device.

- Put in place life cycle planning for all endpoint devices that are owned by the HDO to include approaches for procurement, deployment, support and retirement. Cost capping for end user supplied devices should be in place and also follow a life cycle plan.

- mHealth benefits should be assessed. Results and lessons learned should inform future investments.

13. Conclusion

Infoway believes that mobile devices will continue to increase their footprint in HDOs and eventually replace conventional PCs for many routine functions as well as enabling new capabilities. The ability to access electronic patient records, order diagnostic tests and prescribe medications via smartphones and tablets, at any time and from anywhere, is a game changer for the way clinicians practise medicine. As the technology spreads, there will be a multitude of opportunities for Canada's health community to implement strategic initiatives to proactively address some of the nation's most pressing health care issues.

Clinicians have been quick to adopt mobile devices and medical apps and as a result they are driving a choice oriented model of mobility computing. *Infoway* encourages HDOs to focus on mobility vision, strategy and enterprise scope requirements and policy initiatives before procuring or adopting technical solutions in an effort to catch-up and placate end user demands.

Business leaders' attention will also need to focus on key challenges of governance, regulation and privacy of personal health information.

Infoway hopes that this white paper has provided enough context and meaningful information to contribute to strategic discussion about the approaches to the adoption of mobile computing in the health care sector in Canada.

14. List of Abbreviations

3G	Third generation of mobile telecommunications technology
API	Application programming interface
BCG	Boston Consulting Group
BYOD	Bring Your Own Device
CEO	Chief executive officer
CIO	Chief information officer
CMIO	Chief medical information officer
CT	Computed Tomography
COTS	Commercial off-the-shelf
CPOE	Computerized physician order entry
EHR	Electronic health record
EHRS	Electronic health record solution
EMR	Electronic medical record
FHIR	Fast Healthcare Interoperability Resources
HDO	Health delivery organization
HIS	Hospital information system
HL7	Health Level 7
HTML5	Hypertext mark-up language 5
ICT	Information and communication technology
IEEE	Institute of Electrical and Electronics Engineers
iEHR	Interoperable electronic health record
iOS	iPhone operating system
ISO	International Organization for Standards
IT	Information technology
LDAP	Lightweight directory access protocol
LTE	Long term evolution
MDM	Mobile device management
PACS	Picture archive and communication system
PbD	Privacy by design
PC	Personal computer
PHI	Personal health information
P&S	Privacy and security
RCT	Randomized controlled trial
RFID	Radio frequency identification
SaaS	Software as a Service
SMS	Short message service
TRAM	Transverse Rectus Abdominis Myocutaneous
WCH	Women's College Hospital

15. Contact

Infoway established the Emerging Technology Group (ETG) in 2011 to identify and guide the use of information and communications technologies (ICTs) in health care innovation. The ETG's role is to identify and evaluate emerging technologies, and mature technologies that haven't been fully applied, that look most likely to provide significant benefits to our health care system and the health of Canadians.

This white paper is part of an ETG white paper series which aims to provide information and analysis that could benefit those who make decisions about technologies for health in Canada.

For more information about the ETG and its work, contact ETG@infoway-inforoute.ca or visit our website.