IT Consumerization:
A Case Study of BYOD in a Healthcare Setting

Sarah Marshall

" *Any change, even a change for the better, is always* "
accompanied by drawbacks and discomforts.

Arnold Bennett (1867–1931)
Novelist

The ubiquity and utility of mobile devices in the consumer domain has led organizations to consider the benefits and challenges of allowing their employees to BYOD, or "bring your own device". The consumerization of information technology is a natural transition considering that devices are now commonplace in the personal lives of employees; however, despite the potential benefits to both the organization and employees, the use of employee-owned devices raises issues relating to security, governance, processes, and even organizational culture.

This article focuses on the implementation of BYOD in a healthcare setting. First, the challenges of implementing BYOD in the healthcare industry are examined. Next, a case study of The Ottawa Hospital is developed to illustrate the practical benefits and hurdles that must be overcome when hospital staff begin using consumer IT devices in the workplace. Finally, recommendations are offered to help healthcare organizations develop and implement a successful BYOD strategy.

Introduction

IT consumerization, or the use of consumer products or technologies in the workplace, is an emerging trend in many industries today. Organizations choose to allow and even encourage their employees to "BYOD" (i.e., bring your own device; tinyurl.com/csmwf6e) in an effort to cut costs and increase employee engagement. When employees use their own smartphones, laptops, or tablets in place of distributed devices owned by their employers, they no longer have to carry multiple devices for work and personal use, and they no longer have to learn how to operate various makes and models of technologies.

As indication of the scale of opportunities, consider that, in Canada, there were 17,350,000 subscriptions for mobile devices in 2012 (Euromonitor International, 2013; tinyurl.com/lcde9pu), and it is expected that over 1 billion tablets will have been sold worldwide by the beginning of 2016 (Rafalin, 2012; tinyurl.com/ou7yhsh). Thus,

organizations that are considering a BYOD implementation are likely to find that a great many of their employees already have their own mobile devices that could be used in the workplace.

A survey conducted by Dell (2013; tinyurl.com/oyv7zpz) found that companies that have implemented BYOD have realized a 74% productivity increase. In a hospital, such productivity increases could be seen, for instance, when tests are ordered online by a nurse and a physician must also log in to the system to provide approval. Without mobile devices, physicians typically have to compete for shared desktop computers or return to their offices to approve requests on their own desktop computers, thereby increasing the likelihood of further delays due to interruptions, emergency meetings, etc. With mobile devices, and especially BYOD, physicians can instantaneously approve tests or even order tests themselves, thereby minimizing the wait time for the patient and minimizing time required for follow-up by the nurses.

IT Consumerization: A Case Study of BYOD in a Healthcare Setting

Sarah Marshall

Access to real-time information also ensures that all clinicians have the most current patient data, which is necessary for effective decision making (Rafalin, 2012; tinyurl.com/ou7yhsh). But, there are also benefits for patients, for example, who can easily be shown up-to-date images on a mobile device to better understand their condition or recovery. Of course, such benefits could be realized with hospital-owned mobile devices, but a hospital's efficiency and capacity to deliver these benefits is enhanced by BYOD.

However, there are a number of challenges to overcome when employees use their own devices, including security, compatibility, and data-sharing issues. These challenges are further elevated in the healthcare industry, where patient confidentiality is paramount. In this article, these challenges will be examined, and then a case study will provide a real-world example of a hospital providing mobile devices to its employees and then evaluating additional support for employee-owned consumer IT devices. Finally, recommendations will be offered to healthcare organizations considering support for BYOD.

BYOD Challenges in Healthcare

The key challenges for BYOD in a healthcare setting are introduced below. Although most of these challenges are relevant to the implementation of mobile devices in healthcare generally, in many cases the challenges are exacerbated by the introduction of employee-owned devices.

1. **Security:** the most critical risk factor for organizations implementing BYOD is the risk of security breaches. In healthcare, this risk is often focused on the security and privacy of patient information. The Ponemon Institute reported that, although 81% of healthcare organizations store sensitive patient data on mobile devices that are either owned by the hospitals or its employees, 49% of these organizations do not provide any security for that data (Rafalin, 2012; tinyurl.com/ou7yhsh). Furthermore, phishing scams (tinyurl.com/48zm2) are not uncommon in the industry, and employees are not always cognizant of how to detect them (Rafalin, 2012; tinyurl.com/ou7yhsh). Organizations are able to apply strict firewalls and security measures to their own devices; however, BYOD users are reliant upon their own security mechanisms and may be more exposed to viruses or malware if their own settings are not as strict.

2. **Governance:** for a BYOD program to work effectively, standardized protocols and clear guidelines for both employees and IT staff must be put in place. A survey by KnowBe4 and ITIC (2012; tinyurl.com/qzojgky) found that 71% of businesses that permit employees to BYOD have no official policies, which may prove confusing for employees and increase the risk to the organizations.

3. **Legislation:** in healthcare, there are strict regulations that companies must adhere to with regards to personal health information. For example, in Ontario, Canada, the Personal Health Information Protection Act (PHIPA; tinyurl.com/qy7pzno) and other associated laws provide stringent rules, including hefty fines that are levied whenever a organization's device is lost or stolen (Inside Counsel, 2013; tinyurl.com/k5axvdd). Technology exists to remotely "wipe" a device by deleting its data; however, this technology requires the device to be registered, and employees must weigh the benefits of using their own device at work against the need to comply with the organization's policies on the use and configuration of such devices.

4. **Device type:** an organization may limit the types of devices employees can use as BYOD (Meneghetti, 2013; tinyurl.com/luaklyl). An organization may stipulate that only devices from a particular manufacturer are allowed, either because of security risks, hardware interoperability concerns, or a requirement for particular applications that only run on particular devices. At The Ottawa Hospital in Ottawa, Canada, only Apple devices, including iPads and iPhones, are currently used, in part because the mobile versions of the organization's clinical and electronic health record applications were developed for Apple devices only (tinyurl.com/qz9er9l). As an example of security risks, McAfee reported a 76% increase in malware on Android devices in 2011, which calls into question the security features of the device itself (Euromonitor International, 2013; tinyurl.com/lcde9pu). The availability of devices in a particular form factor may also play a role: although Apple only has about a 20% volume market share of Smartphones, they have an approximately 50% volume share of tablets (Euromonitor International, 2013; tinyurl.com/lcde9pu). These considerations may affect an organization's decision of whether or not to support employee-owned devices; they must balance the desire to support a wide range of devices against interoperability and security

IT Consumerization: A Case Study of BYOD in a Healthcare Setting

Sarah Marshall

needs. Also, they must consider the affordability of certain device types and the wishes of their employees to own particular devices. A related challenge is that BYOD programs have the potential to discriminate against those employees who cannot afford to purchase their own devices. BYOD is based in the assumption that employees are able to (and want to) purchase required devices and maintenance.

5. **Internet dependency:** the high dependency of mobile devices on Internet access requires effective contingency planning in the event of Wi-Fi downtimes or spikes in demand. In a hospital, not being able to access patient files in a time of crisis can be the difference between life and death. Furthermore, the use of employee-owned devices may overwhelm Wi-Fi networks due to their ease of transportation. Currently, the locations of computer workstations in hospitals are typically fixed, such as within certain units or rooms, so that the network and Wi-Fi demand in a given area is predictable and can be managed easily. An abundance of freely moving devices would likely change the Wi-Fi demand dynamics as staff move about the hospital with their devices over the course of a day.

Case Study: The Ottawa Hospital

The Ottawa Hospital (TOH; ottawahospital.on.ca) is the largest teaching and acute care hospital located in Eastern Ontario, Canada, and it is part of the Champlain Local Health Integrated Network (LHIN). Three previously individual institutions, the Civic Hospital, the General Hospital, and the Riverside Hospital were amalgamated in 1999 with the intention of providing patients with full care solutions. As such, services or specialties were able to be fully consolidated to one facility/location; this was a strategic move that enabled all relevant staff, equipment, and supplies to be located in one area. For example, all cancer care including research, surgery, chemotherapy and radiation, appointments, diagnostic imaging, and laboratory services are located at the General Campus. Staff at the hospital total approximately 12,000, including approximately 4,000 nurses, 1,400 physicians, and 900 residents. Additionally, as a teaching hospital, there are many residents and students that come to the organization for specialty training. As the largest hospital within the Champlain LHIN, TOH maintains some of the main repositories for documents, including patient history in their electronic health record system and diagnostic im-

ages in their picture archiving communication system. For these reasons, enabling clinicians to access healthcare information from any device connected to the Internet, whether a desktop computer in an office or a handheld mobile device is imperative.

Mobile Devices at The Ottawa Hospital

The traditional method for healthcare documentation and administration has always been based in paper – paper charts, paper order forms, and paper summaries of tests and procedures performed. In an attempt to become a word-class healthcare organization, ideally ranked in the top 10% in North America, TOH decided to focus on many goals, including quality and safety of care. To ensure high quality and safe outcomes for patients and also to remain on trend in business, TOH has begun to digitize their tasks. For the most critically ill patients, healthcare organizations experience approximately 1.7 medical errors per day (Maslove et al., 2011; tinyurl.com/kjnrfyj), such as when staff fail to administer medicine at the appropriate time or order incorrect tests. To reduce the likelihood of error, improve efficiency, and provide higher-quality healthcare, digitized systems have been or are continuing to be implemented to allow clinicians to view diagnostic test images on mobile devices, order tests from those mobile devices, an enable instant approval of requested orders. TOH has chosen to implement a computerized system that enables physicians to order tests using mobile devices, which they can also use to view the results.

To enable clinicians to use the newly implemented digital systems, TOH chose integrate mobile devices into their infrastructure. They chose Apple's newly released first-generation iPad device as their starting point because it provided an extremely portable device – as opposed to a laptop or a "workstation on wheels" (WOW) – that still had a sufficiently large screen. However, due to privacy considerations, a single iPad was registered to each physician. Although costly, this approach meant that a device could be remotely wiped in the event it was lost or stolen, and it also allowed additional security measures unique to the individual to be installed on the device. A pilot program with a select group of users enabled support services to learn how to manage unexpected issues. The success of the pilot program encouraged the organization to move forward with this strategy, the benefits of which are described in the profile of the TOH's experience on the Apple website: apple.com/ca/ipad/business/profiles/ottawa-hospital/

IT Consumerization: A Case Study of BYOD in a Healthcare Setting
Sarah Marshall

BYOD at The Ottawa Hospital

The computerized physician order entry system was evaluated in the summer of 2013, with an emphasis on the impact on employees and how the system may have changed routine practices. The research yielded two results that are relevant to BYOD.

First, although the iPads were initially made available only to physicians and residents, nurses also perceived value in accessing patient information, ordering tests, and communicating with physicians using mobile devices. However, providing iPads to each nurse would be extremely costly, and the sharing of devices between shift workers might not be practical. A potential solution is to allow nurses to use their own devices as a BYOD extension of the existing mobile system.

The second result highlighted a more critical issue. Some residents complete what is known as a "visiting elective", where they come to TOH for a one- to four-week rotation in an area of specialty. As part of their duties in caring for patients, these residents must access patient information and order tests as required; however, because they will be at the organization for only such as short time, they are typically not provided with full access to computer systems, nor are they provided with an iPad. Instead, they may rely on other staff members to access the systems on their behalf. But, these residents can end up in situations where they are the on-call resident for an overnight shift. If a patient's status becomes critical, the on-call physician or resident is expected to order the required test using the computerized physician order entry system. Until recently, visiting elective residents were unable to complete this task on their own, but TOH is now providing visiting elective residents with access to TOH applications, even though they are not being provided with one of the hospital's devices or mobile access.

Prior to the pilot run with iPads for physicians, Apple devices were not supported at TOH. As of August 2012 at least, the hospital's policies still had not been amended to include statements of support for staff using Apple devices, and therefore compatibility and functionality were not guaranteed. Second-generation iPads were provided to staff prior to completion of full testing, which concerned some of the Citrix developers because they had not fully tested the device with current applications. Finally, requests by individual employees to participate in BYOD have increased steadily

since the introduction of iPads at TOH. BYOD iPads are now supported, but the current program will only provide access to non-sensitive data, and users must register their devices with the identity and access management group. However, some prominent clinicians, mainly physicians, have signed non-disclosure agreements and can therefore access all data, including sensitive data, on their own iPads. However, they must permit TOH to wipe their device should it be lost or stolen. This access is not common practice, and employees are not encouraged to bring their own devices. If they do bring their own devices, they may be able to connect to the internet, but they are not able to log into patient file databases.

At TOH, the vision, security systems, and policies are not yet in place to fully support BYOD technologies. However, their early experiences with mobile devices have helped achieve two of their most valued goals: i) to become a paperless, digitized workplace, and ii) to provide timely, accurate, world-class care for patients (tinyurl.com/qz9er9l). BYOD has the potential to be the next step in the radical transformation the hospital is embarking upon.

Implementation Recommendations

Although challenges remain, the early experiences with mobile systems and BYOD at TOH have been encouraging. Should any healthcare organization such as TOH want to implement a full BYOD program, the following recommendations are offered:

1. Senior management and IT professionals must work collaboratively to design an appropriate mobile device policy that details codes of conduct and expectations. All staff must be made aware of these policies and the potential risks of BYOD to both the organization and the employees themselves.

2. Robust security systems and contingency plans must be implemented, taking into consideration any additional risks associated with employee-owned devices. At TOH, for example, the staff already use two-factor authentication grid cards, but security tokens may be required to provide enhanced security for a BYOD program.

3. Management must anticipate changes in workflows and routines and institute corresponding organizational change initiatives.

IT Consumerization: A Case Study of BYOD in a Healthcare Setting

Sarah Marshall

Conclusion

As the experience of TOH demonstrates, IT consumerization can present challenges to organizations on two related but distinct levels: i) supporting consumer mobile devices in the workplace and ii) supporting employee-owned devices in the workplace, or BYOD. In both cases, the organization must put in place the necessary technical infrastructure to support mobile devices; in the case of BYOD, the organization must implement an additional layer of policy and technical support to manage the risks to privacy and security.

With the ongoing emergence of IT consumerization, the question is not whether or not to BYOD, but how best to manage its implementation to realize its benefits while minimizing its risks. In a healthcare setting, the security and privacy challenges of BYOD are paramount, and yet, the potential benefits of allowing employees to use consumer IT devices are tangible because they can impact not only the productivity of hospital employees but also the health of the people under their care. The case study examined here illustrates that the healthcare industry is making concrete progress, and we can expect to see an increasing presence of consumer IT at the bedside and throughout our hospitals.

About the Author

Sarah Marshall is a Systems Operator at The Ottawa Hospital, and she recently received her MBA in Change Management from Carleton University's Sprott School of Business in Ottawa, Canada. She also holds a Bachelor of International Business from Carleton University.