Bring Your Own Device:
How this is changing the Health Workplace

A Review of the Literature

Introduction

The boundaries between home and work continue to blur for many people these days. We are more connected more often and our choice of technology becomes a reflection of how we see ourselves (Schmidt, 2012). The culture of IT is shifting rapidly, driven largely by the smartphone and tablet revolution initiated by Apple which has led to the consumerisation of IT. The users now have the latest cutting edge technology and they want to use it in their workplace (Bradley, 2013).

"Bring Your Own Device" (BYOD) as a named concept is quite recent. It was first described at Intel corporation around 2009 when it was noticed that increasing numbers of employees were bring their own equipment and in particular mobile devices, and wanting to connect them to the corporate networks (Harkins, 2013). From around 10% of all employees using their own devices in 2010 it is expected that 70% of Intel's employees will have their own devices in use for at least some of their work by 2014. A similar picture is emerging in most industries and the health industry is no exception.

The purpose of this review is to look at the literature related to BYOD to identify key issues for health providers. The factors that have made BYOD a pressing issue in the corporate world are creating a similar demand in the Health environment. This review will identify these factors and highlight similarities as well as differences related to the unique complexity and additional security needs of Health systems.

Literature Review

A review of the relevant literature was conducted using a number of methods. As this topic is relatively recent in origin I expected that there could be some difficulty in finding many references in the health literature so a broad search strategy involving a number of methods was planned.

Medscape Search

The terms BYOD and "bring your own device" did not produce any relevant results using MedLine despite date and subject filtering.

The following MESH terms were all used on their own and with sub categories and filtering.

- Cellular phone
- Mobile computing
- Mobile health
- Telemedicine
- Telehealth
- Computers handheld

The search terms were also combined using Boolean operator AND. Initially only dates from 2011 to the current date were used as I anticipated that there would be very little relevant

literature prior to this. I subsequently expanded the search to 2009 to the present due to limited results.

Google Scholar

A search was conducted using Google Scholar using the same terms as the MedLine search above. The terms BYOD or "bring your own device" on their own and in combination with Health returned over 400 results of varying relevance.

Standard Google Search

A Search was conducted using standard Google using the same terms as above and produced many recent results mostly on information technology sites and blogs.

Internal Resource Search

The topic was discussed with the Chief Information Officers of Canterbury and Waitemata DHBs to determine if any policy documents existed or if not if there were plans to implement policy. Potential and likely approaches as well as trials and pilot testing related to the topic were also discussed.

Method

I found a surprising lack of relevant literature on the subject of clinicians providing their own devices within their workplaces in the health journals during the search. There is an abundance of literature on the utilization of tablets and mobile phones for clinical monitoring, data access, education and communication which suggests that these new technologies and devices are widely accepted. There is little comment however on the use of clinicians providing their own devices for these purposes despite this being a strong possibility.

In contrast, reference to BYOD can be found in many technology news sites on the internet and more formally in journals devoted to information technology and management including the health industry. This suggests that BYOD is viewed primarily as an information technology challenge rather than a healthcare provisioning issue. The review is therefore focused primarily on sources of information outside of the medical literature. Most of the discussion where dates exist is within the last two years. This indicates that the topic is an emerging and escalating issue, in fact it might be described as a "hot" topic that is generating considerable debate.

A total of 37 abstracts or articles were reviewed during the search and seventeen articles were downloaded with citations to Endnote for further review. Fifteen of these are cited in this review

While analyzing the articles I identified the following general themes which I grouped and used as a basis for the discussion.

- The inevitability of change
- Expectations of usability
- IT support for practice
- Corporate, personal and patient risk

- Information security
- Loss of control
- Responsibility
- Support factors
- Cost factors
- Management
- Mitigation factors

Discussion

Fighting the inevitable?

Personal devices are already in the workplace and this is a trend that is impossible to stop. Rather than attempting to stop BYOD in its tracks the only way forward is to embrace it and learn how to manage it (Gilbert, 2012).

At one point in time the organisation provided the necessary tools for your job, but now it is equally likely that some of the tools are user owned. People like their own devices, they choose them for their own purposes, pay for them and treat them with pride of ownership. They would rather use devices that they enjoy owning than the devices that the organisation provides. It can be argued (Bradley, 2013) the people work more effectively and productively with equipment that they have chosen themselves more so than equipment that is forced upon them by the organisation.

There is a sense that as people become attached to their own personal devices they are less willing to learn or use new devices that are not selected by them personally (Miller, 2012). When Apple iPhone and iPad's came on the market the company vigorously evangelised their use in health practice and this has led to demand from clinicians to allow their use in the work environment. As the mobile device market has evolved other devices have entered the space.

The explosion of personal devices has also had a significant impact on user expectations for software. The consumerisation of devices has led to a consumerised perspective on software interfaces. Many of the systems in use in health organisations are elderly with distinctly "industrial" graphic user interfaces that are ill suited to use with modern devices and use patterns. Meneghetti (2013) recommends that whenever services or systems are being replaced or upgraded that mobile optimization and a native "app" approach is taken. This fits well with an increasingly ambulatory workforce carrying their own devices.

Opportunities

The advantages to having anytime, anywhere access to information are described by Schmidt (2012) as obvious. The ability to access a variety of information sources, decision support tools, patient records and email while on the move can increase efficiency and improve collaboration. This is particularly so as most hospital records move to electronic formats. Not having immediate access can lead to delays in treatment decisions (Larner, 2012). Personal portable devices can be key to enabling a rapid transition to the paperless workplace.

Mobile applications can improve safety by enabling instant access to decision support tools. Meneghetti (2013) states 60% of physicians report avoiding at least one adverse drug error a week when using a drug information app. The implication for safer care, reduced risk and therefore reduced costs to the organization are large.

Clinicians are generally resistant to the idea of carrying multiple devices when a single device can be used for both person and professional roles. They value the flexibility of and convenience of having a single device for shared use. BYOD may help retain and attract employees as well as improve employee's creativity satisfaction and productivity (Gilbert, 2012). There may also be benefits from reduced helpdesk requests and reduction in IT spending on devices. This may be offset however by new costs brought about by the demands of managing BYOD on the corporate network

Ultimately one of the major benefits that arises when enabling BYOD in the workplace is that requires the cooperation and involvement of clinicians with the IT department, working together rather than against each other (Wood, 2012). This integration of purpose can have a profound positive effect on both sides of the fence.

Risks

A number of writers warn of the potential risks involved with BYOD. A study by the U.S. Department of Health and Human Services' HIPAA breach site stated that to date, of the 364 data breaches affecting 500 or more individuals, the vast majority have involved lost or stolen laptops, flash drives, or other mobile gear (cited in McGee (2011). These events typically followed the loss or theft of the devices. Data breaches are certainly topical in New Zealand, have a large impact on public confidence in health systems and are costly, distracting and demoralizing to the organization as well as damaging to the health consumer.

Mobile apps may not have security built into them. The security needs of the health care organization are not necessarily a priority for an app developer (Goedert, 2013) and depending on the function of the app this may impact the ability to allow its use in the health environment.

Being able to use your own device is not the same as being required to provide your own. This has the potential to become a vexed issue as expectations change over time. Where will the costs of providing the device or data transmission fall?

Traditional network management practices in Healthcare meant the organization "owned" the desktop and exerted total control over access mostly by limiting use to trusted logins. BYOD requires new models of access control based not just on who is requesting access but also what is requested and where the request is coming from (Mansfield-Devine, 2012). This adds considerable complexity to the task of securing information. Similarly the variety of different devices currently available and the increasing variety of new devices becoming available makes it harder to support. This and the sense of loss of infrastructural control is very worrying to those responsible for managing health IT systems and networks. It is not surprising therefore that CIOs are taking a very cautious approach to the introduction of BYOD (Schmidt, 2012).

Mitigation

A variety of measures and strategies are recommended for managing deployment of a BYOD strategy. Thomson (2012) describes the need for cooperation and dialogue between users and IT to enable a framework that permits the adoption of new technologies in an acceptable and secure way.

Not having a policy for BYOD is described by Narisi (2013) as a common mistake. He cites a SANS institute survey of 650 IT professionals in 2012 that found only 38% of organisations had a policy in place. He recommends that a policy should specify details for the key elements below:

- What devices and mobile operating systems are approved for use on the network
- What security features and settings must be enabled for a device to have access
- What types of data the employee is allowed to store on a personal device
- What apps employees can and cannot install, and
- What actions the organization is allowed to take in terms of managing and monitoring a personal device.

Striking the correct balance in management strategy requires taking into account the need to be as non-invasive as possible while still meeting legal, security and privacy needs (Crowell, 2013). With that in mind there are a number of practices that can help mitigate risk. Schmidt (2012) recommends classification of data to ensure access is appropriate to the user and encryption of all sensitive information. He also advises proactive traffic monitoring for threats, prompt response to threats and constant testing and probing for weaknesses. Limiting data storage time on devices and allowing no clinical data to be left when off the network can considerably reduce exposure (McGee, 2011).

Mobile Device Management (MDM) is promoted by some as a solution to the problem. There are potential problems with MDM solutions, firstly being too restrictive can negate the benefits of having BYOD in the first place and secondly some solutions can be readily disabled by users. The ideal solution may be complete separation of workspace and personal space on a device and newer solutions are emerging such as VMware Horizon and Citrix XenMobile that offer that possibility (Samson, 2013) as well as the ability to remotely wipe stored data in the event of loss or theft.

Conclusion

Despite the paucity of literature on the subject in health journals this is an important area for health IT that warrants further study and is overdue for a more solidly constructed research base.

BYOD is here to stay, it's not a passing fad. Health organizations need to determine the best strategies to handle this while keeping the balance between the ever evolving expectations of their users and the security, confidentiality and privacy requirements of the organisation.

Successful BYOD implementation can improve workflows and clinician access to clinical and decision support information as well as improving patient care and clinician satisfaction. To

make it work it needs active dialogue between clinicians and IT to get the right compromises to ensure workable solutions are chosen.

References

Bradley, T. (2013). Pros and Cons of Bringing Your Own Device to Work, from http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html

Crowell, C. (2013). These are the top 5 BYOD issues facing the healthcare industry, from http://venturebeat.com/2013/04/26/top-5-byod-issues-facing-healthcare-industry/

Gilbert, J. B. (2012). Bring Your Own Device to Work. Retrieved from http://www.lexicon-systems.com/pubs/itinsight/ITInsight1208.pdf website:

Goedert, J. (2013). Mobile device management software: the answer to BYOD? *Health data management, 21*(2), 32-, 34, 36 passim.

Harkins, M. (2013). Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices Retrieved 10/06/2013, from http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264

Larner, S. (2012). Smartphones and tablets in the hospital environment. *British Journal of Healthcare Management, 18*(8), 404-405.

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security, 2012*(4), 14-17. doi: http://dx.doi.org/10.1016/S1361-3723(12)70031-3

McGee, M. K. (2011). How Secure Are Your Clinicians' Mobile Devices? *InformationWeek Healthcare,* from

http://www.informationweek.com/healthcare/mobile-wireless/how-secure-are-your-clinicians-mobile-de/231903089

Meneghetti, A. (2013). Challenges and benefits in a mobile medical world: Institutions should create a set of BYOD guidelines that foster mobile device usage. *Health management technology, 34*(2), 6-7.

Miller, K. W. (2012). BYOD: Security and Privacy Considerations. *IT professional, 14*(5), 53-55. doi: 10.1109/mitp.2012.93

Narisi, S. (2013). Top 3 BYOD policy mistakes healthcare organizations make, from http://www.healthcarebusinesstech.com/byod-policy-mistakes/

Samson, T. (2013). VMware and Citrix aim to simplify BYOD Retrieved 12/06/2013, from http://www.infoworld.com/t/mobile-device-management-mdm/vmware-and-citrix-aim-simplify-byod-213188

Schmidt, J. (2012). Not Your Parents' Workplace Anymore- Managing the New Security Realities of BYOD. *Security (Newton, Mass.), 49*(9), 25.

Thomson, G. (2012). BYOD: enabling the chaos. *Network Security, 2012*(2), 5-8. doi: http://dx.doi.org/10.1016/S1353-4858(12)70013-2

Wood, A. (2012, August 2012). BYOD: the pros and cons for end users and the business Retrieved 10/06/2013, from http://www.bcs.org/content/conWebDoc/47519