12-3-2014

BYOD in ehealth: Herding cats and stable doors, or a catastrophe waiting to happen?

Krishnun Sansurooh
Edith Cowan University

Patricia A H Williams
Edith Cowan University

DOI: 10.4225/75/5798284331b46
3rd Australian eHealth Informatics and Security Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

BYOD IN EHEALTH: HERDING CATS AND STABLE DOORS, OR A CATASTROPHE WAITING TO HAPPEN?

Krishnun Sansurooh[1] Patricia A H Williams[1,2]
[1]Security Research Institute, and School of Computer and Security Science
[2]eHealth Research Group, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
[1]k.sansurooah@ecu.edu.au, [2]trish.williams@ecu.edu.au

Abstract
The use of personal devices in the work environment has crossed the boundaries of work and socially related tasks. With cyber criminals seriously targeting healthcare for medical identity theft, the lack of control of new technologies within healthcare networks becomes an increasing vulnerability. The prolific adoption of personal mobile devices in the healthcare environment requires a proactive approach to the management of Bring Your Own Device (BYOD). This paper analysed the current state of the problem and the challenges that this creates in an environment that has stringent privacy and security requirements. The discourse demonstrates that the issue is not solely technology based and requires a broader approach that is inclusive of technology yet needs an expansive and socially based perspective. Until the use of mobile technology outside the BYOD environment is understood better, definitive guidance for managing BYOD in healthcare will not provide sufficient and acceptable protection, although it is a sound starting point. It is imperative that healthcare rapidly catches up with BYOD use and steps up to the challenge of embracing the technology and human behaviour associated with its user, otherwise, the 'horse will have bolted' before any control can be established.

Keywords
Bring your own device, BYOD, healthcare, risk assessment, security awareness.

INTRODUCTION

Bring your own device (BYOD) refers to the use of personally owned computing devices in the workplace for connectivity to the secure organisational network, and access organisational applications and resources. BYOD has become widespread in corporations, hospitals and universities, which permit users to access the organisational network using a wide range of personal devices (ACMA, 2013). The use of devices such as laptops, smartphones, and tablets, has wide appeal and value, in the familiarity of use, and access to a diverse range of personal and work-related applications and data. BYOD is in stark contrast to IT departments mandating specific hardware and technology, and is fuelled by the advent of Apple's iPhone, and subsequently the iPad (Maas360, 2014). From the user perspective, it is frustrating to know that a particular given task can be accomplished in a faster or easier way using an alternative Web browser, operating system, or application, and users' perceive they are handicapped by "supported products" dictated by the IT department. Interestingly, it is IT professionals, opting to upgrade sooner and self-manage to get the benefits of new versions of products (Jones, 2012), that have led this adoption.

"A striking 81 percent of healthcare providers allow employees to use their own mobile devices to connect to the hospital network, and more than half of employees take part in the BYOD movement". (Ponemon Institute, 2014). It is this integration of personal devices with the work environment that crosses the boundaries of work-personal communication and tasks. Even in institutions where the IT department still decree specific operating systems, hardware platforms, and mobile devices, rogue employees have worked around those requirements to get the job done (Crank, 2014).

One of the issues with BYOD in an environment predominantly unaware of the security risks and not proactive in controlling the use of personal devices, is a lack of appropriate policy for BYOD (Curtis, 2014). It is unfortunate that organisations, up to 70% in the UK, do not have BYOD strategies or policies in place, yet do not prevent employees using their own devices. With cyber criminals taking healthcare seriously for targeted medical identity theft, the vulnerability of using mobile devices in healthcare organisations becomes more difficult to control (Institute for Health Technology Transformation, 2014). The attacks are more prevalent, having doubled in the last three years (Ponemon Institute, 2014), and it is reported that 43% of identity theft in 2013 was medically related (Ollove, 2014). The emergence of attacks on health data are now common in the media, and involve both security breaches and data loss (Gold, 2014; Mearian, 2012;Munro, 2014).

The overburdening of Chief Information Officers and increasing legislation means that addressing BYOD is yet another aspect of security and privacy that is often too difficult for healthcare organisations, particularly smaller healthcare entities such as primary care providers. More problematic is the hospital environment where multiple users require immediate access and multiple IT-networks are required. For instance, the requirements include administration, patient and clinical networks, integration of medical devices, complexity access management where transfer and storage of medical data is undertaken. Scalability of such networks, and the number of authorised users, represents an additional layer of complexity in the management of the clinical network. Therefore, the addition of BYOD poses a massive potential security threat as well as a major security management issue for IT departments in trying to adhere and integrate BYOD into an already complex network.

This paper discusses BYOD use in healthcare and highlights the risks this setting presents. In addition, the parameters that influence the security of BYOD and the multiple contributing factors of integrating mobile technology and applications with potentially sensitive information into healthcare IT-networks are presented. The analysis of these issues results in a discourse on the types of recommendations that could be applied to the management of BYOD within the healthcare environment. It further suggests how security and flexibility may be maintained in the transition from traditional information access to BYOD.

ADJUSTING TO A MOBILE WORLD

In healthcare, particularly secondary and tertiary care, mobility and access to multiple workstations is essential to support effective workflow. Traditionally this is facilitated by organisational dictation of applications, software, and hardware, together with administrator passwords centrally controlled, albeit with poor control of access (Filkins, 2014). Indeed, there is a growing expectation and demand for freedom to use personal devices for work, accessing the healthcare network to perform daily tasks (Free, 2014). Users are extremely resourceful and if new technology can assist and make their role more effective, then this will be adopted, even if the use is ‘under the radar’. This shift in acceptability means that organisations would rather not fight the use of personal devices for work yet have not taken the initiative to attempt manage this use, or do not have the capability to manage its use. There is an inherent difficultly in managing the use of technology that is not in the complete control of an IT department (Longo, 2013). The transition to a BYOD environment means major adjustment for some organisations, rather than managing a small, predictable set of devices and configurations. BYOD presents a complex and dynamic landscape, with many different models of laptops, tablets, and smartphones, running Windows, Android, or other operating systems.

BYOD RISKS IN HEALTHCARE

The general risks that apply across all domains include device security, application security, and managing the environment in terms of interfacing to existing systems. Previously, mobile devices were relatively straightforward to manage and secure as they consisted of a uniform distribution of device types, often from a single manufacturer or brand, that had limited or no access to organisational data. This allowed consistent application of security policy controls, often through a unified management interface supplied by the manufacturer. BYOD fundamentally changes this architecture as users bring in their own devices of various makes and models, and varying hardware and operating system combinations. As a result, basic security controls may not be applied consistently and effectively across the multitude of devices. This may occur even when a functional Mobile Device Management (MDM) product is in place, as operating system or app-specific vulnerabilities may be able to circumvent existing controls on the device.

The risks specific to healthcare, in addition to other risks associated generally with mobile devices, include capability, information sensitivity, integration with workflow, and the use of associated integrated services and applications. Indeed the context of use is “often invisible, mutable and without the necessary security warnings” as the contextual environment is not self-evident (Longo, 2013), particularly in a strong commnuity of practice based setting, as healthcare is.

Device Security

The primary aim for organizations is to deliver business value. Locking down mobile devices and prohibiting the use of personal devices may ameliorate some security risks, however policies that are too restrictive will influence the adoption or encourage workarounds. The general risks relating to securing mobile devices can be categorised as lost and stolen devices, physical access, device ownership, ‘always on’ with increased data access, and lack of awareness. There are numerous examples of realisation of these risks in healthcare involving patient sensitive information (EYGM, 2013; Williams, 2009; U.S. Department of Health & Human Services, 2013).

Application Security

Mobile applications (apps) have accelerated the use of mobile devices. From embedded computing applications such as real-time location identification and mapping apps to social networking; from productivity tools to games; apps have largely driven the smartphone revolution. While apps demonstrate utility that is bound only by developer imagination, it also increases the risk of supporting BYOD devices in an organisational environment. The two general security risks are supplemented by an additional and important, patient safety risk:

1. Mobile malware are apps with code embedded that can compromise the security of the device or the data stored on the device.

2. App vulnerabilities exist where they enable access to organisational data. The risk of app vulnerabilities is accentuated when the IT department does not manage devices, as this model forgoes remote administrative capabilities and the associated control.

3. Third-party software that provides specific functionality outside the host application and database requires secure interoperability with agreed consistent and accountable interfaces. The vulnerabilities that such software present are in the form of buffer overflows, input manipulation, and application authentication. Such third party software is parasitic in nature as the host system is not aware of, nor has an agreed consistent interface to, the application. In a context where assurance of patient safety should outweigh all other issues concerning the use of software in healthcare, this is problematic. Whilst, "the importance to the healthcare environment is in the benefits that such third party software can provide in both the integration of electronic services and in providing facilities such as clinical audit tools and healthcare practice analysis" (McCauley & Williams, 2011), international concern is widespread. This concern is demonstrated by increasing engagement and development work at International Organisation for Standardisation (ISO) in projects related to the safety of mobile devices, medical devices, embedded and stand-alone health software. These include *ISO 25238 Health informatics -- Classification of safety risks from health software; ISO 17791 Health informatics -- Guidance on standards for enabling safety in health software; and ISO/IEC 82304 Health software -- Part 1: General requirements for product safety*.

Managing the Environment

A Gartner survey predicted that by the year 2017, half of employers would require employees to supply their own device for work purposes (Gartner, 2013). A BYOD environment has more variability in the hardware and software versions of devices holding administrative, patient/medical, and organisational data, and providing access to this data. This will further decrease the ability of MDMs to manage and consistently apply technical security policies to the endpoints. This variation in platforms also complicates device wiping when phones are lost, replaced, resold, or upgraded by users, or when there is a change in mobile service provider. Hidden costs and user expectations highlight the importance of choosing the right governance and support models.

Capability

There is a general lack of capability in many healthcare organisations concerning security and the protection of information. (Williams, 2011). This situation is compounded by poor design of security measures within the complex environment of healthcare (Coles-Kemp & Williams, 2012), and exacerbated by a lack of appropriate documented mobile strategy, policy and procedures to manage mobile and BYOD use (Slabodkin, 2012).

Information Sensitivity

The personal nature of health information requires a higher level of protection than other less sensitive information. The technological advances and the increasing jurisdictional health and privacy regulations are increasing the cognizance of the susceptibility of sensitive medical and patient information to breaches (Williams & Hossack, 2013). In Australia, the new Australian Privacy Principles (Office of the Australian Information Commissioner, 2014) demand greater oversight and protection of health related data both in transit and at rest. The nature of mobile device functionality in storage and data transfer mean demonstrable alignment and conformity to this legislation.

Workflow into Service Delivery and Clinical Care

The recognition of the benefits and hindrances in the use of mobile devices in terms of both regulatory frameworks and clinical care workflow can assist in embracing BYOD safely. Delivering the right information about the right patient at the right place and time is paramount to high quality healthcare (Prgomet, Georgiou, & Westbrook, 2009). The problems with traditional access to clinical information using tethered computers is that it does not allow mobility to where the patient is situated, and mobile paper based charts do not allow for real-time accessibility. There is evidence that the use of mobile devices, improves patient outcomes, for instance through the prevention of medication errors due to the increased accessibility of information at the patient bedside (Moyer, 2013).

Integrated Services and Applications

The increasing bandwidth and imaging application capabilities is one example where sharing information is now possible using mobile devices (Donovan, 2013). This raises a number of issues in relation to confidentiality of the data and subsequent patient privacy. The use of medical image sharing, for a 'second-opinion, particularly in emergency departments is not uncommon. For instance, an image taken on a mobile phone (even with the patient's consent) presents a number of insecure points of failure. Firstly, the transfer of the image using text messaging or email is not a secure transfer; the management of the image sharing once sent is not recorded; secure deletion of the image from the mobile phone; protection of the image at the receiver's end; secure deletion of the image from the receiving device; and so on. In addition, if the image is used as part of a diagnosis, it should also be added to the patient's health record. Secure solutions for the transfer and deletion of each part of this workflow scenario exists however the problem is the management of the whole workflow process and its component parts as the data is recorded, accessed and stored with multiple people in multiple locations physically and logically.

Another issue that is applicable to all organisations who allow BYOD is that of automatic device backup to the cloud. This has additional implications for the location of information stored overseas and the requirement of equivalent privacy legislation under the Australian Privacy Principles (Williams & Maeder, 2014). Whilst a private cloud is a sound idea for healthcare data, the issue with user owned mobile devices is that the cloud provisions are often set up automatically i.e. to the platform manufacturer cloud service, for which the user has little or no control.

PROTECTION, GOVERNANCE AND COMPLIANCE

In addition to the protection of BYOD and integration into the organisational usage parameters, the issues of governance with regard to privacy need consideration. Privacy legislation in many countries, such as the Australian Privacy Principles (Office of the Australian Information Commissioner, 2012), and the EU Privacy Directive ("EU Poised to Propose 24Hour Breach Notification Data Privacy Rules 379540" 2012), provide additional legislation with ramifications for mobile device management. One approach to address these issues is to employ a structure of standards and best practices that acknowledge the complexity of the environment. This includes the Safety of Health IT-Networks in the ISO 80001 series, and the *ISO 17791 Health informatics -- Guidance on standards for enabling safety in health software*. Hence, an initial approach to BYOD policy, (to begin to 'herd the cats'), is a set of best practice BYOD guiding principles that specifically address the idiosyncrasies of healthcare.

Healthcare BYOD Guiding Principles.

Guiding principles are not prescriptive, and rather than suggest policy content, they provide a framework to encompass both the technical (usually exclusive) and social (inclusive) necessities. The following guiding principles transfer the focus from traditional command and control to a flexible policy-based network provisioning that can support personal mobile devices, whilst being cognizant of the environment. These are grouped below (to promote initial discussion and deconstruction of the complex environment of use) into policy, technical (configuration and monitoring) and social categories (Table 1).

Table 1 BYOD Guiding Principles

Policy	
1	*Adopt a structured, standards-based and device agnostic approach to BYOD protection*. Investigation into user and organisational needs, within a wider environment of information sharing in healthcare, is required. For example, physicians may feel that iPads are preferable in the hospital because they can be sterilised. This sterilisation is required to prevent the spread of nosocomial infections. Environmental and security requirements can be mapped to international standards, and consideration of technical solutions such as MDM applications (including remote wiping facilities) may fulfil technical protection requirements of such standards.
2	*Ensure a balanced approach to protection and accessibility*. Understanding and provision for complex healthcare workflow is vital.
Technical (Configuration & Monitoring) Various technical measures are underpinned by initial configuration and monitoring activities.	
3	*Establish a mobile device and permissible operating systems list, which can be endorsed on the network.*
4	*Establish the mandatory applications (or prohibited) for each device*.
5	*Establish a user group list*
6	*Define who, what, where and when of network access*. Role based access is vitally important in the management of healthcare information and meeting jurisdictional privacy legislation.
7	*Audit authorized and unauthorized devices, and authorized and unauthorized users*
8	*Continuous vulnerability assessment and remediation*.
9	*Information protection – encryption for data at rest and data in motion.* Encryption of data at rest is particularly important on mobile devices that have little other protection. In reality the best option, and to meet jurisdictional privacy requirements, personal health information should not be stored on a mobile device.
10	*Integrating network segmentation and data segmentation.* Using application virtualisation facilitates increased control whilst decoupling from device dependency.
Social	
11	*Educate users about BYOD risk and BYOD policy*.

Whilst these guidelines provide a general framework to guide initial control of the BYOD environment, what is arguably more important, and should drive further investigation and design of effective solutions for healthcare, is investigation and a full understanding of how users of BYOD interact with the wider environment outside the healthcare environment. The simplicity and convenience of gaining a second opinion, for instance by texting or emailing a photo of a patient's condition, means that an understanding of the information flow involved in such an exchange is needed to be able to design effective security solutions. This task should also include how to include information collected outside the usual clinical system into the patient record, as well as the persistence of any information held on a mobile device.

CONCLUSION

The guiding principles proposed provide an inclusive approach to management of BYOD rather than the traditional technologically based approach. The issue of privacy of information is front and centre of the risks that all patient health data are subjected to. Healthcare organisations need to embrace that patients and healthcare providers want to use mobile devices for connection, communication, and for accessing services. It is in this

failure that the issues of privacy get lost in security measures to protect devices and data confidentiality. The intangible nature of data maligns its value, which in the case of health related data, is not the 'value' of the data itself but its usefulness in clinical decision-making. The use of this data and how it is handled is paramount to managing patient privacy. As Hossack (2014), points out, privacy is a contextual concept. In healthcare when a person is well privacy is important, when the same person is ill, privacy is less important than accessing relevant information for the best health outcome.

With the rapid expansion of mobile devices entering the workplace, it is unrealistic to ignore BYOD use, or use a blanket approach of preclusion, as users will continue to use non-compliant devices to access the network with or without organisational recognition and permission. It is unfortunate that as Forrester's study (2013) suggests, that US information workers revealed that 37% are employing new technologies before formal permissions or policies are instituted. Add to this the context of use, necessary workflow, impact of communities of practice, and the lack of security capability, and the resulting optimisation in the secure use of BYOD will take time to develop.

Addressing the management and control of BYOD in healthcare is a challenge. It requires a new approach to security in healthcare, which encompasses a shift in the technical paradigm making full use of virtualisation and data segmentation, whilst including the pragmatic approach to seamless integration into a complex workflow.

The proliferation of device use without initial control has meant a major vulnerability exists to the healthcare industry. As the examples demonstrate, this vulnerability is being exploited and needs to be contained, even though this maybe 'closing the stable door after the horse has bolted'. The recommendations made in this paper are a preliminary investigation into an issue that will only become more widespread. It provides a starting point to develop solutions that can be readily adopted in healthcare, where the paternalistic approach and interruption of workflow that limits health service delivery is resisted. The adoption of multiple methods of collection of, and interaction with, health information using a diverse range of technology presents new and major challenges for the healthcare environment. Whilst these include the challenges found in other organisational environments, the diversity, lack of awareness and critical workflow factors in healthcare provide a scenario more resembling herding cats that managing data.

REFERENCES

ACMA. (2013). *Communications report 2011–12 series Report 3 - Smartphones and tablets take-up in Australia.* Canberra: Australian Communications and Media Authority.

Crank, C. (2014). *Tips for mitigating BYOD security risks.* Retrieved from http://www.baselinemag.com/security/tips-for-mitigating-byod-security-risks.html

EYGM. (2013). *Bring your own device security and risk considerations for your mobile device program*. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

Filkins, B. (2014). *SANS Health Care Cyberthreat Report* (pp. 42). Retrieved from http://pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf

Forrester Research, Inc. (2013). *2013 Mobile workforce adoption trends.* Retrieved January 7, 2014 from http://www.vmware.com/files/pdf/Forrester_2013_Mobile_Workforce_Adoption_Trends_Feb2013.pdf

Free, J. (2014). Real-world BYOD security. *Health Management Technology, 35*(3), 14-17.

Jones, J. (2012). *Beginner's guide to BYOD (Bring Your Own Device).* Retrieved February 9, 2014 from http://blogs.technet.com/b/security/archive/2012/07/18/beginner-s-guide-to-byod-bring-your-own-device.aspx

MaaS360. (2014). *The ten commandment Of BYOD.* Retrieved from http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf

Coles-Kemp, L, & Williams, P.A.H. (2012). Security specialists are from Mars; healthcare practitioners are from Venus: the case for a community-of-practice approach to security architectures for healthcare. In P. A. H. Williams & L. Coles-Kemp (Eds.), *1st Australian eHealth Informatics and Security Conference (pp. 35-41)*. Perth: ECISRI - Security Research Institute, Edith Cowan University.

Curtis, J. (2014). How blocking BYOD leads to shadow IT. *Computer Business Review*. http://www.cbronline.com/news/tech/cio-agenda/the-boardroom/how-blocking-byod-leads-to-shadow-it-4346795

Donovan, F. (2013). BYOD trend increasing need for security vigilance in health care. *FierceMobileIT*. Retrieved from http://www.fiercemobileit.com/story/byod-trend-increasing-need-security-vigilance-health-care/2013-04-12

EU Poised to Propose 24Hour Breach Notification Data Privacy Rules 379540. (2012, 2012/01/24/). *eWeek*.

Gold, A.. (2014). *Most health IT execs unprepared for a data breach.* Fierce Health IT. Retrieved from http://www.fiercehealthit.com/story/most-health-it-execs-unprepared-data-breach/2014-02-03

Hossack, E. (2014). Lost in translation: privacy perceptions and software development. *Privacy Unbound iappANZ,* (55), 5.

Institute for Health Technology Transformation. (2014). *Healthcare security: 10 Steps to maintaining data privacy in a changing mobile world.* Retrieved from http://ihealthtran.com/healthcare-security.

Longo, B. (2013). Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime. *Legal Information Management, 13*(2), 119-123. doi: http://dx.doi.org/10.1017/S1472669613000285

McCauley, V., & Williams, P.A.H. (2011). Trusted interoperability and the patient safety issues of parasitic health care software. In P. A. H. Williams (Ed.), *9th Australian Information Security Management Conference* (pp. 189-194). Perth: secau- Security Research Centre, Edith Cowan University.

Mearian, Ls. (2012). *'Wall of Shame' exposes 21M medical record breaches. ComputerWorld.* Retreived from http://www.computerworld.com/s/article/print/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches

Moyer, J.E. (2013). Managing mobile devices in hospitals: A literature review of BYOD policies and usage. *Journal of Hospital Librarianship, 13*(3), 197-208. doi: 10.1080/15323269.2013.798768

Munro, D. (2014). Assessing the financial impact of 4.5 million stolen health records. *Forbes*, 4. http://onforb.es/1tAbzMt.

Office of the Australian Information Commissioner. (2012). *Mandatory data breach notification in the eHealth record system*. Australian Government Retrieved from http://www.oaic.gov.au/news/consultations.html#ehealth_dbn.

Office of the Australian Information Commissioner. (2014). *Privacy fact sheet 17: Australian Privacy Principles*. http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

Ollove, M. (2014, Feb 7, 2014). Nearly half of identify thefts in the U.S. are medical info, *USA Today*. Retrieved from http://www.usatoday.com/story.news/nation/2014/02/07/stateline-identity-thefts-medical-information/5279351/

Ponemon Institute. (2014). *Fourth annual benchmark study on patient privacy & data security*. Retrieved from http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security

Prgomet, M, Georgiou, A. & Westbrook, J. (2009). The impact of mobile handheld technology on hospital physicians' work practices and patient care: A systematic review. *J Am Med Inform Assoc, 16*(6), 792–801. doi: 10.1197/jamia.M3215

Slabodkin, G. (2012). Two-thirds of healthcare organisations lack a written mobile strategy. *FierceMobile Healthcare*. Retrieved from http://www.fiercemobilehealthcare.com/node/9906/print

U.S. Department of Health & Human Services. (2013). *Health information privacy: Breaches affecting 500 or more individuals*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Williams, P.A.H. (2009). Capturing culture in medical information security research. *Methodological Innovations 4*(3), 15-26. doi: DOI: 10.4256/mio.2010.0003

Williams, P.A.H. (2011). Is the biggest security threat to medical information simply a lack of understanding? *Studies in Hhealth Technology and Informatics, 168*, 179-187.

Williams, P.A.H., & Hossack, E. (2013). It will never happen to us: The likelihood and impact of privacy breaches on health data in Australia. In H. Grain (Ed.), *Studies in Health Technology and Informatics* (pp. 155-168). Amsterdam: IOS Press.

Williams, P.A.H., & Maeder, A. (2014). Security and privacy issues for mobile health. In S. Adibi (Ed.), *Mobile Health (mHealth): The Technology Road Map* (pp. [In press]): Springer.