1-1-2012

Mobile Device Management for Personally Controlled Electronic Health Records: Effective Selection of Evaluation Criteria

Murray Brand

Patricia Williams
Edith Cowan University

Originally published in the Proceedings of the 1st Australian eHealth Informatics and Security Conference, held on the 3rd-5th December, 2012 at Novotel Langley Hotel, Perth, Western Australia

MOBILE DEVICE MANAGEMENT FOR PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORDS: EFFECTIVE SELECTION OF EVALUATION CRITERIA

Murray Brand[1], Patricia A. H. Williams[2]
[1]School of Computer and Security Science, Edith Cowan University
[2]eHealth Research Group, School of Computer and Security Science & ECU Security Research Institute,
Edith Cowan University
[1]m.brand@ecu.edu.au, [2]trish.williams@ecu.edu.au

Abstract

Enterprises are faced with the task of managing a plethora of mobile computing devices in the workplace that are employed for both business purposes and private use. This integration can contribute to the demands of security protection and add significant threats to the enterprise. The introduction of the Personally Controlled Electronic Health Record (PCEHR) system is a significant step in e-health for Australia and will likely result in sensitive information being accessed from mobile computing devices. Mobile Device Management (MDM) offers a potential solution to manage these devices, however there is a variety of vendors with a range of solutions. This paper presents preliminary research into a generic methodology that could be used to assist the enterprise in the MDM selection process particularly when mobile devices will eventually integrate with the Australia's PCEHR.

Keywords

Mobile device management, MDM, PCEHR, evaluation criteria, e-health.

INTRODUCTION

The consumerization of information technology (IT) is witnessing the integration by users of their personally owned consumer mobile computing devices with work based functions. This is reported to be increasing productivity, but introduces various security threats to the enterprise (Marcos, 2012). Threats to mobile devices can include malware, loss or theft, communication interception, exploitation and interception (Juniper Networks, 2011). Mobile Device Management (MDM) offers features to assist in configuring mobile devices such that they more closely comply with usage policies (Withers, 2012). A list of features available in MDM can include remotely locking and wiping lost or stolen devices, application management, password enforcement, inventory and asset management, security and policy compliance, remote location of lost devices, integration with enterprise services such as e-mail and certificate authorities, backup and restore services. A variety of MDM solutions are offered by vendors, with a diversity of architectures and specifications. The selection of an optimal solution for any given scenario could be assisted by the use of quantitative methods.

In July 2012 Australia commenced use of a Personally Controlled Electronic Health Record (PCEHR) system as part of a national e-health initiative. The PCEHR is an electronic health summary stored and shared in a distributed network of connected systems and will be able to be accessed by users and user authorized healthcare providers. The significant advantage of the PCEHR is that healthcare providers will be more suitably enabled to optimize treatment advice (National eHealth Transition Authority, 2012). Mobile computing offers great benefits to the heath care industry, but the mobile devices employed are subject to the same significant threats that all mobile devices are potentially exposed to. MDM offers a possible solution to assist with the compliance of policy when mobile devices integrate with the PCEHR system. The objective of this paper is to present preliminary research that is being conducted towards publishing a methodology to develop applicable evaluation criteria to select a suitable MDM specifically for integration with the PCEHR.

MOBILE DEVICES IN THE ENTERPRISE

The threat landscape to mobile computing devices is evolving at a rapid rate. This includes application based threats such as malware, vulnerable applications, and threats to privacy. Web based threats include browser exploits, phishing scams and drive-by-downloads. Mobile computing devices are also vulnerable to network based threats such as network based exploits via WiFi, BlueTooth and cellular interfaces. Such portable devices are easily lost or stolen and can contain not only personally identifiable information, but also commercial and intellectual property information (Lookout Mobile Security, 2011).

Mobile computing devices such as smart phones and tablets are rapidly becoming integrated into the workplace and offer the advantage of increased productivity. It is highly likely that these devices are part of the Bring Your Own Device (BYOD) revolution where employees incorporate their own, consumer computing devices into the workplace for both work and personal use. Thomson (2012) points out that IT department need to "enable the chaos" that results from this integration and that creative and flexible solutions are required from IT to maintain security, provide support and enable access to collaborative technologies.

Cerrato (2012) asserts that there are downsides to allowing physicians and clinicians to connect their personal mobile devices to hospital and office systems, including usability factors such as poor screen layout as well as significant security issues. Poor screen layout for example, may result in data not being displayed correctly and that this could result in threats to patient safety. This is significant because it emphasizes why the selection of mobile computing devices is critical. In addition, BYOD introduces new threats to the security of information, including the threat of data loss. Mobile devices can operate outside the security perimeter and defences of the enterprise. If a device is lost or stolen, information on the device is likely to be very accessible. The Henry Ford Health System, a hospital in Detroit, had a laptop stolen which contained unsecured information of 3,700 patients in September 2010, and an employee lost a flash drive containing information on 2,777 patients in March 2011. In September 2011, an employee at Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan in Philadelphia misplaced a flash drive containing the information of 280,000 members (Horowitz, 2011).These represent only a few examples of such security incidents involving health data. Where we consider the use of BYOD across the various healthcare contexts there are numerous aspects to consider from the security perspective. The basics include deciding what types of devices and platforms will be allowed to access the network. Similarly, decisions on the applications and data that will be accessible must be made, and finally what access control and vulnerability assessment will be undertaken on a continual basis (Bradford Networks, 2012). Whilst approximately 40% of workers are aware there are risks, up to 60% are happy to contravene their organisations policy in order to use their mobile devices (Eddy, 2012). The low level of security awareness and insecure practices by healthcare mobile users with poor or no password protection on these devices are of major concern (Wicklund, 2012). This poses a significant issue if not recognised and regardless of the risks, organisations will be forced to embrace their use and address the security issues.

PCEHR

The PCEHR Concept of Operations document (Australian Government, 2011) explains that the need for a PCEHR system has been defined by the fragmentation of information distributed over a vast number of locations and systems. The objective of the introduction of the PCEHR will be to allow people to have greater access to their own health information and to be able to actively select which health care providers have access to this information. The anticipated benefits described in the Concept of Operations include improved continuity of care for individuals who access multiple health care providers, access to consolidated information about an individual's medicines leading to more effective medication management and empowering individuals to more actively participate in their healthcare. Individuals will use a Consumer Portal to access and manage their PCEHR. Healthcare providers and organisations will be able to access the PCEHR system by accessing clinical systems and alternatively via a provider portal. The PCEHR Act 2012 (Australian Government, 2012a), provides for civil penalties for unauthorised collection of information included in a registered consumer's PCEHR and the unauthorised use or disclosure of such information. In addition, contraventions of the PCEHR Act can be investigated under the Privacy Act 1988 (Australian Government, 2012b). This is significant, because clinicians and practices that use mobile devices are just as subject to the threats all mobile devices users are subject to, and loss or disclosure of information is a possibility.

MOBILE DEVICE MANAGEMENT

A non exhaustive list of features an MDM can include the ability to remotely wipe, lock and/or locate lost devices, install software, push updates and security patches, enforce policies such as password complexity, enforce encryption, disable integrated devices such as cameras and audio recording and enforce authentication.

The Gartner Magic Quadrant Report for MDM software (Redman, Girard, & Wallin, 2011) highlights some of the defining elements of a MDM to be:

- Ability to install, deploy, update, block or delete mobile applications through software distribution.
- Enforce device security, authentication and encryption through security management.
- Develop, control and distribution of policies through policy management.
- Provide inventory management, provisioning and support through inventory management.

- Rate telecommunications services through service management.

As a proposition to apply this into the healthcare environment this paper uses same definition for MDM. A variety of MDM solution architectures are available. The Gartner report continues by declaring that more than 60 vendors offer products and services to manage mobile computing devices in the enterprise. This can include services on-premises, cloud based services, or hybrid systems that contain elements of both. Managed services are also available where the management function is provided by an external party (Wavelink, 2011). On-premises, self-managed solutions likely integrate with existing IT infrastructure that exist within the perimeter network that could include a Certificate Authority, E-Mail servers, domain controllers, enrolment servers and gateways (Microsoft, 2009). Cloud based services in contrast are managed off-premises by a 3rd party and the customer organization uses a web page based interface to enrol and manage devices. With either of these solutions, a software agent needs to be installed on the mobile computing device. This is considered to be either a lightweight approach or a heavyweight approach. The lightweight approach calls the native Application Programming Interface (API) provided by the Operating System (OS) of the mobile and is dependent upon the management features and capability of the API. It cannot completely control the device and user behaviour (Basso & Redman, 2011). The heavyweight approach in contrast, can enforce very strong control of the device because the client software installed integrates more closely with the mobile OS. The tiered nature of this view of possible mobile device solutions is depicted in the matrix diagram of Figure 1.

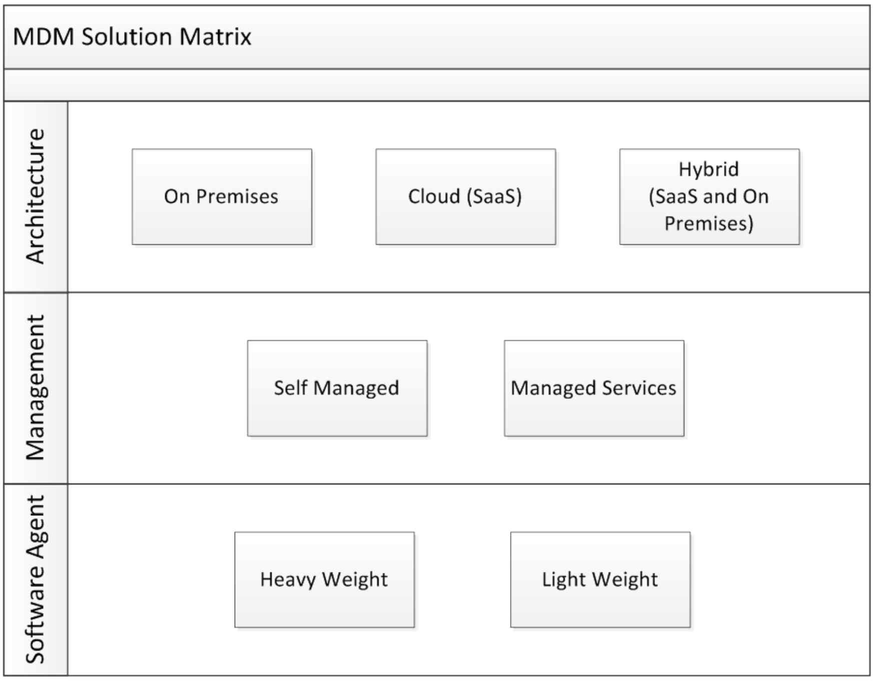

Figure 1. MDM Solution Matrix

The selection of a suitable MDM will depend upon a myriad of factors, defined by the constraints of usage and security policy, law, regulation, compliance, support and risk management within a very dynamic environment where new mobile computing products are being released, new threats eventuate on a near daily basis, and new collaborative and innovative software is being offered to consumers and business users. To this end, this paper postulates that selection of effective evaluation criteria is essential, through the benefit of conducting a formal trade study.

Trade Studies

Trade studies can be used as an objective, structured and quantitative methodology for evaluating potential solutions, architectures and designs, based on a determined set of evaluation criteria. Such studies are beneficial because they justify and document the decision process and assist in selecting the most appropriate option. They help ensure that a rational and unbiased decision is reached and that the decision is defendable.

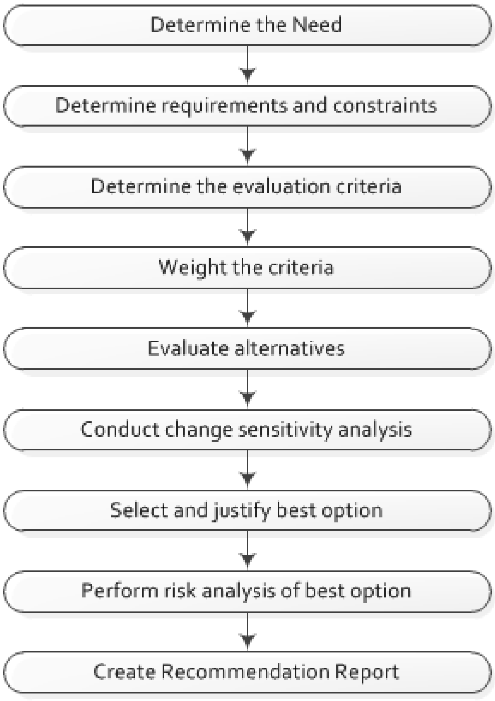
Determine the Need
Determine requirements and constraints
Determine the evaluation criteria
Weight the criteria
Evaluate alternatives
Conduct change sensitivity analysis
Select and justify best option
Perform risk analysis of best option
Create Recommendation Report

Figure 2. Overall Trade Study Flowchart

Figure 2 depicts the overall flow of events for conducting a trade study tailored for evaluating MDM systems for PCEHR, developed from examining a number of engineering publications (Bayuk, 2011; Jamshidi, 2008; Rebovich, 2010). The study is initiated by documenting the need and objective of problem. This is followed by documenting constraints and determination of requirements. The need statement, constraints and requirements can then be used to establish the selection criteria which should be selected to be quantifiable and to be able to be differentiated from each other. The evaluation criteria can then be entered into a table and weighted according to their relative and justified importance. This ensures that the most important criteria have the most effect on the final score. Once the weighting table is created, the vendors' products can then be evaluated. This can be achieved by vendor data, analysis, measurement, simulation or some other quantifiable method. When this phase is completed, a sensitivity analysis can then be conducted and is used to assess the sensitivity of each option to small changes in the evaluation criteria or in the uncertainty in the measurements. Once the best option is selected, a risk analysis is conducted to determine if there will be any adverse consequences to selecting the option. The release of the final report concludes the trade study analysis and should provide the documentation of the entire process.

Whilst this gives a solid basis for the development of process, what also needs to be applied is the contextualisation of process, what also needs to be applied is the contextualisation of the flowchart into the target domain. This is particularly important for the healthcare environment where sensitivity and trust are important factors (Williams, 2008). In an environment where a potentially vulnerable national system is included, it is vitally important to put in place effective protective procedures.

MDM AND THE PCEHR TRADE STUDY

In the healthcare environment the users are not, as a rule, technology savvy or well versed in security (Williams, 2009). Whilst this situation is not peculiar to healthcare, the importance of this is that the lack of control over BYOD, the lack of awareness of security, and the difficultly in integrating security into healthcare workflow, together with the personally sensitive nature of the information means that management of mobile devices should be a priority. Selection of the most appropriate MDM system for PCEHR could be assisted by employment of the following process.

Determine the Need

The initiating step in the process is to define the overall need of the system, to identify the users, applications and data sources that can be used to bind the overall scope. This could include the PCEHR records, the need to interact with distributed systems, databases, provider portals and specific e-Heath software applications used by clinicians, health care workers and clients. This could be assisted by interviewing stakeholders, creation of use case diagrams and developing problem statements. Standards pertaining to collaborative care communications, diagnostic messaging, electronic health records interoperability, health concept representation, information security, messaging and communication (HL7), patient administration messaging, prescription messaging, supply chain and telehealth may need to be identified and examined. Privacy law and the PCEHR Act will need to be examined. Existing security and usage policies need to be located and analysed. The results of this and all steps need to be documented. If any gaps are identified between security requirements and existing policies they must be rectified. An MDM system provides the opportunity to centrally manage and enforce policy and the foundation of the need has to be established before the following steps are conducted.

Determine the Requirements and Constraints

Requirements identification is used to formally define the attributes and capability of the system to achieve an objective. It defines the what, the how well, and under what conditions the attribute or capability of the system must provide. A system is built on requirements, which in turn are developed after analysing the needs of the system. If the system is not defined in terms of requirements, it is highly likely the delivered system will not meet the needs of the users. The requirements can be in the form of functional requirements, which define the functions of the system, and performance requirements which describe how well the functional requirements must perform. It is critical that the requirements are verifiable by a single test, be concise and unambiguous, be implementation free and that they are necessary.

Determine the Evaluation Criteria

The evaluation criteria must be developed such that the various alternatives can be differentiated without bias and relate directly to the defined requirements, which in turn were developed from the need. It is important that the criteria be able to be effectively measureable, and that the stakeholders and evaluators agree and understand them.

Weight the Criteria

The evaluation criteria should be weighted according to their importance with respect to their comparative importance such that the most important criteria have the highest weighting and the least important criteria have the lowest weighting. The resultant effect is that the most critical criteria have the greatest influence on the resultant decision. The criteria and their weightings are entered into a table or spreadsheet and the vendors products are assigned a score against the criteria. It is very important that the criteria selected be measureable and quantifiable so that the resultant decision is sound.

Evaluate Alternatives

The quantitative evaluation of the alternatives may be conducted by analysing vendor data, actual measurement of real systems, evaluation of demonstration software and hardware or by estimations. Once the vendors products are evaluated, the resultant score for each product can be determined, with the objective being that the most highly scored products are the ones likely to be the most suitable product or option, to meet the needs of the needed system.

Conduct Change Sensitivity Analysis

A sensitivity analysis is conducted to determine how sensitive the selected options are to small changes to the weights of the evaluation criteria. The technology of mobile devices with respect to hardware, software and mobile operating systems is evolving at a very rapid rate. Confidence in the resultant selection can be expressed if small changes in weightings cause small changes in the highest scoring selections.

Select and Justify Best Option

The option that receives the highest score, and is least sensitive to small changes in the weightings of the evaluation criteria may likely be justifiable as the most desirable option.

Perform Risk Assessment of Best Option

A risk assessment of the best option should be performed to determine if there will be any adverse consequences if the selected option is implemented.

Create Recommendation Report

The recommendation report can then be collated that presents the findings of the selection activity and documents the history and justifiability of the selection process as well as identification of any identifiable adverse consequences.

CONCLUSION

There is no doubt that the healthcare workforce, like many others, will embrace the use of mobile devices in their work environment and fuel demand for the acceptance of this. MDM systems offer the opportunity to enforce security policies via a centralized point of control and management. A variety of architectures and solutions are available, and this paper recommends that formal methods of evaluation of MDM systems are used to select the most appropriate one. Further refinement of this evaluation criteria methodology for the new e-health environment is needed, but what is significant is that it can be based on established sound principles as is developed in this paper. The engagement of a documented and structured selection process to evaluate MDM solutions for PCEHR will assist in making an unbiased, defendable decision based on quantitative methods. With current data breach legislation under discussion in Australia, its impact and the need for improved IT governance will be needed to provide assurance and protection.

This application and modelling of the use of MDM to the healthcare environment is to demonstrate a proof of concept. This preliminary research will be further extended using a case study and appropriate use cases from healthcare, in collaboration with other experts in the field of healthcare security architecture.

REFERENCES

Australian Government. (2011). Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record System. Retrieved from http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr-document

Australian Government. (2012a). PCEHR ACT 2012. Retrieved from http://www.comlaw.gov.au/Details/C2012A00063

Australian Government. (2012b). Privacy Act 1988. Retrieved from http://www.comlaw.gov.au/Series/C2004A03712

Basso, M., & Redman, P. (2011). Critical Capabilities for Mobile Device Management. Retrieved from http://www.gartner.com/technology/reprints.do?id=1-16U0UOL&ct=110801&st=sg

Bayuk, J. L. (2011). Systems Security Engineering. *Security & Privacy, IEEE, 9*(2), 72-74.

Cerrato, P. (2012). Why BYOD Doesn't Always Work In Healthcare. *InformationWeek*. Retrieved from http://www.informationweek.com/healthcare/security-privacy/why-byod-doesnt-always-work-in-healthcar/232601666

Horowitz, B. (2011). Data Breach Affects 2,777 Henry Ford Health System Patients. Retrieved from http://www.eweek.com/c/a/Health-Care-IT/Data-Breach-Affects-2777-Henry-Ford-Health-System-Patients-415908/

Jamshidi, M. (2008). System of Systems Engineering : Innovations for the Twenty-First Century, Retrieved from http://ECU.eblib.com.au/patron/FullRecord.aspx?p=380453

Juniper Networks. (2011). Mobile Device Security - Emerging Threats, Essential Strategies. Key Capabilities for Safeguarding Mobile Devices and Corporate Assets. Retrieved from http://www.juniper.net/us/en/local/pdf/whitepapers/2000372-en.pdf

Lookout Mobile Security. (2011). 2011 Mobile Threat Report. Retrieved from https://www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf

Marcos, C. (2012). Embracing BYOD. *SC Magazine, 23*(8), 26-27.

Microsoft. (2009). Mobile Device Manager System Overview. Retrieved from http://technet.microsoft.com/en-us/library/dd261798.aspx

National eHealth Transition Authority. (2012). What is a PCEHR? Retrieved from http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcher

Rebovich, G. (2010). Enterprise Systems Engineering : Advances in the Theory and Practice. Retrieved from http://ECU.eblib.com.au/patron/FullRecord.aspx?p=555713

Redman, P., Girard, J., & Wallin, L. (2011). Magic Quadrant for Mobile Device Management Software. Retrieved from http://www.sap.com/campaigns/2011_04_mobility/assets/GartnerReport_MDM_MQ_April2011.pdf

Thomson, G. (2012). BYOD: enabling the chaos. *Network Security, 2012*(2), 5-8.

Wavelink. (2011). Selecting the right mobile device management solution: On-premise, managed service or SaaS. Retrieved from http://www.wavelink.com/whitepapers/avalanche-delivery-whitepaper.pdf

Williams, P. A. H. (2008). When trust defies common sense. *Health Informatics Journal, 14*(3), 211-221.

Williams, P. A. H. (2009). Capturing culture in medical informatics security research. *Methodological Innovations, 4*(3), 15-26.

Withers, S. (2012). Mitigating mobile information security risk with mobile device management (MDM) Retrieved from http://www.voiceanddata.com.au/articles/52333-Mitigating-mobile-information-security-risk-with-mobile-device-management-MDM