UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Developing a Mobile Device Management (MDM) Security Metamodel for Bring Your Own Devices (BYOD) in Hospitals

Sambo Sisala & Siti Hajar Othman
Information Assurance and Security Research Group (IASRG)
School of Computing,
Faculty of Engineering,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
ssisala2003@yahoo.com, hajar@utm.my

Submitted: 07/09/2020. Revised edition: 12/10/2020. Accepted: 13/10/2020. Published online: 19/11/2020
DOI: https://doi.org/10.11113/ijic.v10n2.273

***Abstract*—With cybercrime on the rise, the healthcare environment has been listed as the top 5 of the most targeted industries for information security breaches. This is due to the current migration from physical to Electronic Health Records (EHR). The challenges of controlling the database costs also continue to escalate. As a result, measures such as Bring Your Own Device (BYOD) policies are commonly utilized to minimize costs and create convenience for hospital staff to use a device they are more comfortable with. However, BYOD can be used as a major entry point for gaining access to Health Information Systems (HIS) by cyber attackers/hackers despite the struggles of many hospitals to put in place effective mobile security policies. Several researches have been done to show on how to create effective mobile device BYOD strategies by using device management, data security, medical applications, information technology, education, policy, guidelines and a few others. But there is still a lack of literature about BYOD policy development in hospitals especially when it comes to Mobile Device Management (MDM), policy evaluation, and mobile device evaluation. To help address this issue, an MDM security metamodels has been proposed to help bridge this gap of knowledge between security professionals and shareholders within the healthcare environment. With awareness to the proposed solution, the elementary stage is to identify any existing MDM models that have been created for BYOD in healthcare and use the metamodel to represent some of the important existing concepts. Therefore, the context of this research paper aims to concentrate on improving existing BYOD security policies through the awareness of these existing MDM concepts that are represented through a metamodel syntax. This paper aims to discuss important MDM security concepts from various sources that have been used in healthcare, create a MDM security metamodel prototype called MDMSec ver 1.0 for the healthcare sector, using a selected metamodeling process, and lastly, to validate the prototype metamodel through two validation techniques.**

***Keywords*—Bring Your Own Devices (BYOD), Health Information Systems (HIS), Electronic Health Records (EHR), Mobile Device Management (MDM)**

I. INTRODUCTION

Bring Your Own Device (BYOD) refers to an organizational practice that allows staff members to make use of their personal computing devices to access the organization's network for working purposes (Rouse, 2012). In the context of a hospital, it allows hospital stakeholders (researchers, institutions, communities and individuals) to access healthcare data with their own devices. Statistics taken from a survey, which was conducted on 350 healthcare leaders in 2017, indicated that at least 71% of them allowed BYOD to be used in their hospital in some capacity (Spok, 2017). Consequently, BYOD is also being used as a major point of gaining access to Health Information Systems (HIS). Many hospitals are facing challenges to put in place effective policies to mitigate these risks such as breaches to sensitive data and the numerous threats that come from malicious application. This is mainly due to the difficulties that come with establishing and setting strict personal device regulations that govern the protocols for healthcare workers to be able to access data from health

institutions in a safe manner using their personal devices (Consoltech, 2019).

Some of the difficulties hospitals have with BYOD are due to the security concerns that come with accessing sensitive data. For example, there needs to be clear BYOD policies that will enforce various data security issues, such as: validating the type of data that can be transmitted, applying restrictions on which applications can be used and what can be downloaded, mitigating the threat of introducing malware onto the network through adware, bots, rootkits, spyware, Trojans, viruses and worms, and data theft and privacy violations (Esecurityplanet, 2018). A significant number of these incidents occur within environments where there is a perceived lack of knowledge and understanding towards security risks and 2 where the staff does not proactively take measures to protect their devices, this is a result of an absence of effective BYOD security policies and device management practices (Curtis, 2014). Furthermore, studies have shown examples of how to create BYOD strategies and policies in hospitals using: mobile device management, data security, medical applications, information technology, education, policy, and guidelines, among other things (Kadimo *et al*., 2018).

To help address this issue, Mobile Device Management (MDM) software has been created to assist IT administrators to protect, monitor and implement laptop, smartphone and other devices to ensure that workers do not violate important policies and that the data stays safe. MDM solutions have been around for some time, however, these MDM solutions can still be challenging to implement due to reasons such as: challenges with BYOD, low user experience which can lead to employee frustration and a willingness to avoid using the MDM properly, data loss due to lost devices and theft, and a lack of skilled workers due to low awareness levels about MDM components (Customtec, 2017). Thus, for MDM solutions to work properly, a big factor is that they need to be better understood by all stakeholders before they can be applied more effectively. In addition, to improve the awareness of MDM solutions, security metamodels have been proposed to bridge this gap of knowledge. Metamodels are used for formal naming and defining. They are important because they help us to create models that better study and identify the gaps and challenges that exist in a targeted domain. The context of this research project aims to concentrate on improving existing research on building more improved BYOD security policies though MDM systems. The objective is to explore the effectiveness of existing

MDM security models that have been created in this domain create a prototype metamodel and enhance the metamodel. This paper consists of eight sections, Section I (Introduction), Section II (Project Background), Section III (Project Statement), Project IV (Metamodeling Techniques), Section V (Justification of the Selected Approach in Metamodeling Process), VI (The Metamodeling Process), Section VII (Discussion) and VIII (Conclusion and Future Works).

II. PROJECT BACKGROUND

The reason many hospitals are facing challenges such as how to validate the type of data that can be transmitted, how to apply restrictions on which applications can be used and what can be downloaded etc. is due to the fact that most security experts are lacking of security knowledge of how to create and enforce suitable BYOD security policies to meet the unique needs of their institution (Mace, Parkin and Moorsel, 2010). As a result, hospitals will need to create more robust healthcare BYOD policies (Donovan, 2019). With that said, building more robust policies will require shareholders to have a good understanding of the security concepts as well as having good systems in place that can help to enforce effective security policies that are relevant to the hospital domain. To accomplish this task, MDM security metamodels have been proposed to bridge this gap of knowledge as explained in Section 1.1.

The purpose of this paper is to provide an example of applying knowledge reuse through a unified MDM security metamodel. This research by software engineering practice is called 'Metamodeling' (Brinkkemper, 1996). Through metamodels, information security professionals will be able to utilize these MDM models to answer complex problems and display relationships across the domain. In essence, this is a place where the components of a MDM security domain can be defined in detail. By identifying these components we can create metamodel patterns that help us to understand complex MDM systems by making them easier to represent in models (Brinkkemper, 1996). Therefore, the objectives are listed as follows:

- To identify the important MDM concepts from various models that have been used in healthcare.
- To create a MDM security metamodel for the healthcare sector, using a metamodeling process.
- To validate the prototype metamodel through existing MDM models that have been created using the "Comparison to Other Models" technique.

III. PROJECT STATEMENT

Many hospitals are faced with challenges to put in place effective policies to mitigate the threats that come with BYOD. As explained earlier, some of these threats include introducing malware onto the network, validating the type of data that can be transmitted by a user's device, applying restrictions on which applications can be used and what can be downloaded, amongst other things (Positive Technologies, 2019). Implementing and enforcing effective security policies can prevent many of these threats. MDM systems have been identified as a solution due to their ability to enforce security policies. However, one of the major challenges that come with MDM systems is the lack of understanding about the important components that belong to it and how they work. For this reason, the paper proposes a MDM security metamodel (Identity Management Institute, 2020).

IV. METAMODELING TECHNIQUES

From a practical point of view, no matter which metamodel is used, the sample size and distribution and the difference between the metamodel and the actual feature are always a concern for accuracy. Thus methods were under development that can iteratively improve the accuracy of the metamodel (Dennis and Torczon, 1996). Regardless of which metamodeling technique is used for a specific problem, it is observed that the modeling efficiency and accuracy are directly related to the design space (i.e., the approximation space for metamodels). Therefore, an iterative development technique is advised. However, there are different types of development techniques that can be used as discussed in Table I below:

TABLE I. METAMODELING DEVELOPMENT TECHNIQUES

Metamodel Technique	Process
Blind Kringing	Steps Included: Conduct a background review of the problem domain Collect data of related topics Gathering data and coding it Developing a framework with separated data
Test Driven Approach – Model Development	Steps Included: Identify domain concepts & relations Refine model Write a test model Execute the test model Evaluate (informal) if successful go to step 2, if not go to step 6 Identify refactoring (informal)
Learning by Doing Approach	Steps Included: Knowledge codes are analyzed. Model validation is performed by evaluating the semantic correspondence between the two metamodels. The semantic agreement analysis tests the distances of each build, whether they have counterparts on both metamodels. In design execute a new iteration. The iteration of the metamodel in its creation and refinement process is up to 18 times before the final version is made.
Metamodeling Creation Process	Steps Included: Preliminary observation against problem domain of study. Identifying best collection of models to suit research tasks. Extraction of general concepts. Short-listing candidate definitions. Reconciliation of definitions. Designation of concepts. Creating relationships among concepts. Metamodel validation.

V. JUSTIFICATION ON SELECTED APPROACH IN THE METAMODELING PROCESS (OTHMAN, 2014)

In the creation of a metamodel there are different types of techniques, which can be used. Some of these techniques have been mentioned in Table I such as the blind Kriging (Beer, 2004), the Test-driven Approach (Cicchetti *et al*., 2011), the Learning by Doing Approach (Garcia, 2007), and the Metamodeling Creation Process (Othman *et al*., 2014) are more suitable for the development of a domain model based on the review.

For the purpose of this study, the 'Metamodeling Creation Process' applied by (Othman *et al*., 2014) was used to create the MDMSec model. This technique is chosen and found to be the most effective technique to use in the production of MDMSec based on security because it relies on completeness, performance, correctness, and adequacy in the production of the metamodel (Othman *et al*., 2014).

For instance, in step 1 the process entails that we must identify the best collection of models to suit the research task. In this situation, the chosen models are based on a model selection criterion.

Once various BYOD Security models were identified, they were filtered through a model selection coverage criterion. The basis of this model criterion was established using Guidelines for Managing the Security of Mobile Devices in the Enterprise, this is a publication created by the National Institute of Standards and Technology (NIST). This publication provided four key concepts for establishing MDM Security in an enterprise, including that of a hospital. Furthermore, each of the 30 models were examined based on their frequency coverage to meet these four key concepts (Data Communication & Storage, Application Security, General Security Policies, and User & Device Authentication). For example, the models that listed all four concepts were given a 'YES', while if any model did not meet this criterion of all 4, or failed to mention MDM Security in any capacity, they were excluded from the selection. The higher the value (1 - 4), the higher the completeness. Thus, this is how the 10 models were identified and chosen to represent the MDM Security Metamodel (MDMSec).

VI. THE METAMODELING PROCESS (OTHMAN, 2014)

The Metamodeling process consists of three phases. Phase 1 consists of the Problem Identification Phase, Phase 2, consists of the Metamodeling Development and Validation and Phase 3, and is the application of the MDM Model. These phases can be seen in Fig. 1 (below).

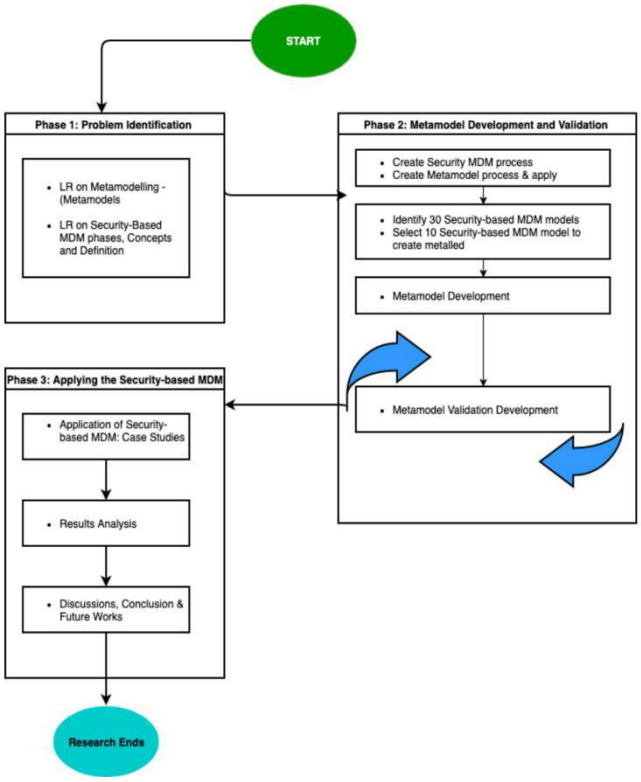

Fig. 1. The Research Methodology in Three Phases

A. Phase 1: Problem Identification

Like many other model design methodologies, the development of this metamodel begins with problem identification. This is because the value of a proposed solution is better understood when the problem is well defined. In fact, the problem identification stage is usually seen as the most important phase of a study. This is because it drives the research questions and processes used to set the framework for understanding the results of the study (Bryman, 2005). The identification of the problem for this paper is the most important part of the study. This reflected on the nature of preserving data security by enforcing security policies through MDM solutions. For example, they explained the need for there to be clear BYOD policies that will enforce various data security issues, such as: validating the type of data that can be transmitted, applying restrictions on which applications can be used and what can be downloaded, mitigating the threat of introducing malware onto the network through adware, bots, rootkits, spyware, Trojans, viruses and worms, and data theft and privacy violations.

These chapters have identified the problem, proposed a solution through the creation of a metamodel (MDMSec) and identified models where the key concepts can be extracted to create this model, and finally mapping out future considerations for the study.

B. Phase 2: Metamodel Development & Validation

This phase of the study focuses on developing the actual model. The important concepts are well defined at this point. Before this occurs, 30 existing models that are related to BYOD Security are examined, where 10 that are related to MDM Security in Hospitals were selected. The selected models also help by providing a basic understanding of the MDMSec domain and the components that are frequently presented through listed concepts. The development process utilized from the beginning to the end was the 'Metamodeling Creation Process' adapted from (Othman *et al*, 2014). This process is defined as an iterative process, this means that the process uses a systematic, repetitive, and recursive process because it involves conducting a sequence of tasks repetitively in an exact same way to refine the model. This process consists of 8 steps, as seen in Fig. 2.

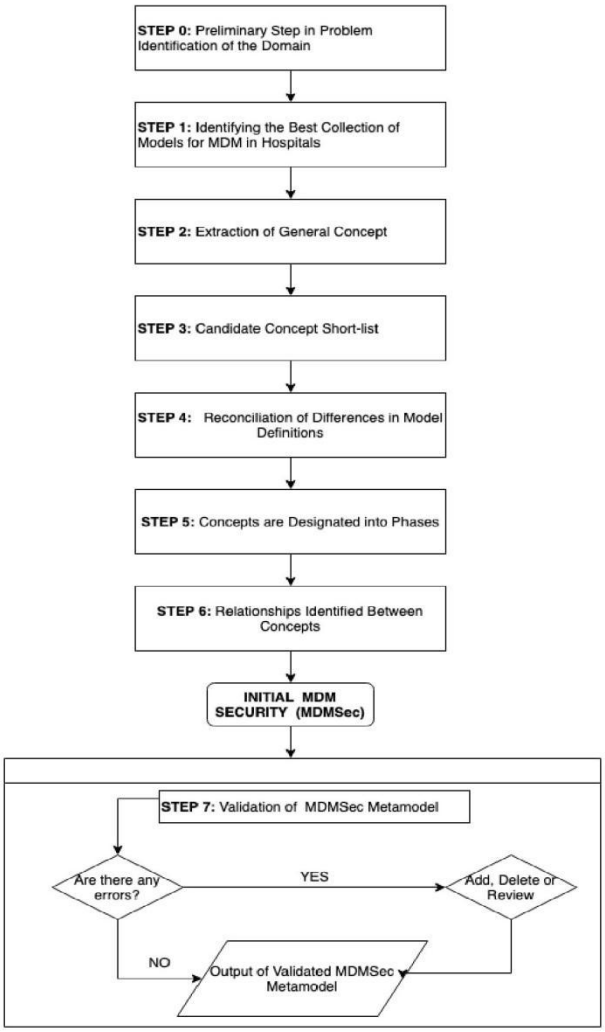

Fig. 2. Metamodel Development & Validation Process

SAs prescribed by Othman *et al*, 2014, the process begins with step 0. This entails identifying the problem. This step is usually conducted in more detail during earlier stages of the study. It relates to a lack of security awareness. Security awareness is a fundamental component of information security. A huge part of security awareness involves understanding. In a nutshell, this is the importance of creating a metamodel for MDM Security. This is because metamodels create a model for people that come from various knowledge backgrounds to better understand the terminology used in a specific domain. In this case, the purpose of this metamodel is to create a knowledge model that even employees' that may not necessarily have an IT background to be able to understand their relationship with MDM and how they affect organization security. Now that the value of metamodels has been explained, the next section aims to explain the importance of having MDM in modern organizations.

1) Step 1 – Identifying the Best Collection of Models from BYOD Models

The metamodeling process begins with Stage 0, which is the Identification of the problem. This step is conducted in the earlier parts of the study and involves the collection of existing BYOD Security models and identifying the best set of models to use to create the metamodel. Once various BYOD Security models were identified, they were filtered through a model selection coverage criterion. The basis of this model selection criterion was established using a Guideline for MDM Security paper, which was a publication by the National Institute of Standards and Technology (NIST). This publication provided four key concepts (Data Communication & Storage, Application Security, General Security Policies, and User & Device Authentication) for establishing MDM Security in an enterprise, including that of a hospital. Therefore, each of the 30 models were examined using a Degree of Confidence (DoC) and given a tick (✓), if all four key concepts were covered with a (✓) then the model was accepted. While the models that did not meet this criterion, or failed to mention MDM Security in any capacity, will be excluded from the selection. Thus, this is how the 10 models were identified. The selected models used for the development of the MDMSec.

2) Step 2 - Extraction of General Concepts

As explained in Step 1, the key concepts were identified using an NIST publication which governs a standard for creating effective MDM Security practices in Hospitals. These concepts can be defined as key/common/general concepts as they are important in creating the metamodel. From these key concepts, we can ensure that we can create a model that is consistent.

3) Step 3 – Candidate Short-listed Concepts

At this point we can gather all the concepts that were extracted and make sure that their definitions are short-listed and can be used to create a common definition.

4) Step 4 – Reconciling the differences between the key concept definitions

Once the process of short-listing concepts has been performed, the next step is to reconcile all the key concepts (Data Communication & Storage, Applications, General Security Policies, and User & Device Authentication) which were identified. The reason for this is because the security MDM models that have been selected were all developed by different stakeholders (researchers, institutions, communities and individuals). Therefore, when the concepts are closely examined we can observe some differences in how they are defined in each model.

5) Step 5 – Chosen Concepts are Designated into Phases

In this step the reconciled concepts from step 4 are assigned to their respective sets and as a result, the focus is placed on putting all the concepts that were extracted to each of the four common concepts (Data Communication & Storage, Applications Security, General Security Policies, and User & Device Authentication). The Data Communication & Storage is the phase that seeks to protect data that is in transit or that is sitting on a storage device. The Application Security phase applies measures of control, through strict security checks as applications have access to sensitive data, and the General Security Policies phase defines the security policies that are put into place as guidelines for improving the behavior and the discipline of the healthcare staff. Lack of such measures leads to misinformation or misunderstanding, which leads to bad practices in security. Finally, the User & Device Authentication phase relates to the process used when a user/employee tries to access the data and they must undergo a verification process that can be carried out on the identity of the user or identity of the device or both.

6) Step 6 – Identify the Relationships between Concepts

In step 6, the relationships between the MDM concepts are determined. To do this the Unified Modelling Language (UML) class has been used to establish the relationships. When identifying relationships there are three types that are used between concepts in a metamodel. These are association, aggregation and specialization.

7) Step 7 - Metamodel Validation

The two techniques used to validate the model are through an Expert Review Technique and a Comparison with Other Models Technique. As the names suggest, the Expert Review takes the feedback of someone that has experience with working or providing a MDM security solution to a hospital. While a Comparison with Other Models technique is accomplished by identifying components or concepts that are missing in an initial model by comparing them against other models that are similar to that domain. In this case, the research will use the most validated model MDMSec V1.1 and identify other relative or similar models, which can be used to enhance it. From the MDMSec V1.1 there were 69 concepts

that were listed and used to create this model. The model was then compared with other existing models to identify any other missing concepts, where an additional 15 concepts were added to enhance it to MDMSec V1.2.

C. Phase 3: Applying the MDM Security Model in a Real Scenario

The purpose of this research is primarily to exchange the knowledge of MDM systems being applied from various models for the Hospital security domain. Through this metamodel we are able to create a unified model language of representation that can be used to share knowledge about the important concepts that exist when managing a BYOD system through the implementation of MDM security. The development of this model should help bring clarity about the existence of these concepts, what they mean, by means of definitions and how they are connected through relationships. This is the knowledge that can help towards improving future BYOD security in a hospital domain. In phase 4, the metamodel can be issued to users to apply it and further validate its effectiveness towards knowledge language distribution.

VII. DISCUSSION

In this paper two validations were performed. First, by using an 'Expert Validation' through a questionnaire and secondly, through a 'Comparison to other Models' technique. For the first validation, two experts have given their feedback through a questionnaire, which was then used to enhance the metamodel from MDMSec v1.0 to v1.1. From the first validation technique ten new concepts were added.

The second validation technique is to analyse publications the publications that were produced by the NIST and NHS. The aim was to identify missing concepts that could be added or modified to enhance the MDMSec v1.1 model from validation v1.1 to v1.2. The results obtained helped to identify fifteen new concepts, which were added to the metamodel. Besides adding new concepts, the overall model was refined to show better clarity. Now that these two validation techniques have been performed the MDMSec v1.2 model looks more refined and clear. However, it is still not as perfect as other BYOD models which can reflect concepts that are suitable for a specific situation or environment. The next chapter of the paper suggests how this study could be used for future works.

VIII. CONCLUSION AND FUTURE WORKS

There is a great potential of using Metamodels as a knowledge base, as identified in this study. However, in view of the study's limitations, the following recommendations are proposed for future research:

- Based on observations and experiences during the process, it can be argued that there is still a need for a better understanding of shareholders' needs, especially when it comes to the health care domain. Future studies should be handled with a more formal and active involvement with health workers as well as security experts.
- Future studies can examine components that could be used to further enhance the model for improved accuracy. Especially because as new security threats are identified, there will always be room for enhancement.
- There are certain technology factors that need to be determined in the planning stage of a future model, this includes determining what kind of devices or operating systems will be permitted to use inside the hospital, what privileges will be provided to different types of employees and which telecommunications provider, authentication software or network security technologies will be used. Choosing the right technology depends on many factors, such as hospital organizational capabilities, end-user experience, clinical workflow integration and compliance with all security requirements for litigation.

In conclusion, the paper aims to execute the development of the metamodel. It validates the metamodel using two validation techniques, firstly, through an Expert Questionnaire and secondly, with a Comparison with Other Models technique. and finally, it concludes the research of the paper and addresses areas for future research within this field of study.

REFERENCES

[1] 42Gears. (2019). Difference between Mobile Device Management (MDM), Enterprise Mobility Management (EMM) and Unified Endpoint Management (UEM). (2019, November 6). Retrieved from https://www.42gears.com/blog/difference-between-mdm-emm-uem/.

[2] BEERS, W. C. M. V. (2005). Kriging Metamodelling for Simulation. PhD, Tilburg University.

[3] Bermell-Garcia, P. (2007). A Metamodel to Annotate Knowledge based Engineering Codes as Enterprise Knowledge Resources.

[4] Beydoun, G., *et al.* (2009). FAML: A Generic Metamodel for MAS Development. *IEEE Transactions on Software Engineering*, 35(6), 841-863. Doi:10.1109/tse.2009.34.

[5] Bobology. (2015, June 24). What is Location Tracking? Retrieved from https://www.bobology.com/public/What-is-Location-Tracking.cfm.

[6] Bradley, T., & Bradley, T. (2015, January 16). Location Tracking in Mobile Apps is Putting Users at Risk. Retrieved from https://www.csoonline.com/article/2871933/location-tracking-in-mobile-apps-is-putting-users-at-risk.html.

[7] Brinkkemper, Sjaak. (1996). Method Engineering: Engineering of Information Systems Development Methods and Tools. *Information & Software Technology*, 38, 275-280. 10.1016/0950-5849(95)01059-9.

[8] Bruce Schneier. (2015). *Secrets and Lies: Digital Security in a Networked World*. Chapter 23. John Wiley & Sons, Inc.

[9] Bryman, B. A., & Social Research. (2005). The Research Question in Social Research: What is its Role? Retrieved from https://www.tandfonline.com/doi/abs/10.1080/13645570600655282.

[10] Buch, N. (2017, December 27). Mobile Device Management Solutions to Achieve Tech-Savvy Healthcare Services.

Retrieved from https://medium.com/mobilock-pro/mobile-device-management-solutions-to-achieve-tech-savvy-healthcare-services-aabf37aba429.

[11] BYOD Security: Understanding Bring Your Own Device Security Risks. (n.d.). Retrieved from https://www.esecurityplanet.com/mobile-security/byod-bring-your-own-device.html.

[12] Cicchetti, A., Ruscio, D. D., Kolovos, D. S. and Pierantonio, A., (2011). A Test-driven Approach for Metamodel Development. Emerging Technologies for the Evolution and Maintenance of Software Models, 319-342.

[13] Columbia University (CU). (n.d.). Who is Responsible for Risk Management. Retrieved from https://finance.columbia.edu/content/who-responsible-risk-management.

[14] Comodo Group. (2019, November 4). What are Android Security Updates? Importance of Security Patches. Retrieved from https://antivirus.comodo.com/blog/comodo-news/android-security-updates-mobile-security-patches-important/.

[15] Consoltech. (2019, April 9). 8 Big Security Threats to Cybersecurity in Healthcare: 2018. Retrieved from https://consoltech.com/blog/security-threats-healthcare-systems/

[16] Curtis, J. (19 August 2014). How Blocking BYOD Leads to Shadow IT. Retrieved from https://www.cbronline.com/news/tech/cio-agenda/the-boardroom/how-blocking-byod-leads-to-shadow-it-4346795.

[17] Customtec. (2017, September 19). The Challenges for Mobile Device Management: CustomTec - IT Professional Managed Services and Cloud. Retrieved from https://customtec.net.au/challenges-mobile-device-management/.

[18] Cuthbertson, A. (2018). Dead People's Medical Records are Being Posted on the Dark Web and Hackers are Making a Fortune, 13 July 2018. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/hackers-dead-people-medical-records-dark-web-cyber-security-data-a8444851.html.

[19] Davies, Islay & Green, Peter & Milton, Simon & Rosemann, Michael. (2007). Analyzing and Comparing Ontologism with Meta-Models. 10.4018/9781591403753.ch001.

[20] Demicoli, C. (2018, January 20). Never Accept a MDM Policy on Your Personal Phone. Retrieved from https://blog.cdemi.io/never-accept-an-mdm-policy-on-your-personal-phone/.

[21] Dennis, J. E., and Torczon, V. (1996). Managing Approximation Models in Optimization. Multidisciplinary Design Optimization: State of the Art, N. Alexandrov and M. Y. Hussaini, eds. Society for Industrial and Applied Mathematics. Philadelphia.

[22] Donovan, F. (2019, June 18). Personal Mobile Device Use Underscores Healthcare BYOD Policy Need. Retrieved from https://hitinfrastructure.com/news/personal-mobile-device-use-underscores-healthcare-byod-policy-need.

[23] Educalingo. (n.d.). TRACKING DEVICE - Definition and Synonyms of Tracking Device in the English Dictionary. Retrieved from https://educalingo.com/en/dic-en/tracking-device.

[24] Enninga, T., Manschot, M., van Gessel, C., Gijbels, J., van der Lugt, R., Visser, F. S., Verhoeven, F., and Godfroij, B. (2013). *Service Design, Insights from Nine Case Studies*. Utrecht: HU University of Applied Sciences Utrecht.

[25] FIJITSU. (2012, October). BYOD: Four Case Studies Show the Reality Behind the Hype. Retrieved from https://www.i-cio.com/strategy/mobile/item/byod-four-case-studies-show-the-reality-behind-the-hype.

[26] Graves. (2015). What is Acceptable Use Policy (AUP)? - Definition from WhatIs.com. Retrieved from https://whatis.techtarget.com/definition/acceptable-use-policy-AUP.

[27] Génova, G. (2009). Modeling and Metamodeling in Model Driven Development. Retrieved from http://www.ie.inf.uc3m.es/ggenova/Warsaw/Part3.pdf.

[28] HealthIT, Improved Patient Care Using EHRs. (2018). Retrieved from https://www.healthit.gov/topic/health-it-basics/improved-patient-care-using-ehrs.

[29] HealthItOutcomes. (2012). National Health Service (NHS) Selects MaaS360 For Mobile Device Management. Retrieved from https://www.healthitoutcomes.com/doc/national-health-service-nhs-selects-maas-0001.

[30] Healthway. (2018, April 25). 5 Surprising Problems with Hospital Privacy (and What You Can Do). Retrieved from https://www.healthyway.com/content/surprising-problems-with-hospital-privacy-and-what-you-can-do/.

[31] Hevner, Alan & Chatterjee, Samir. (2010). Design Science Research in Information Systems. 10.1007/978-1-4419-5653-8_2.

[32] Hexnode. (2019). MDM Healthcare Solutions by Hexnode. Retrieved from https://www.hexnode.com/mobile-device-management/mdm-case-study-brightstar-care/.

[33] Hinkle, D. E., Jurs, S. G., & Wiersma, W. (2003). *Applied Statistics for the Behavioral Sciences.* Belmont, CA: Wadsworth.

[34] Identity Management Institute. (2020). Using Mobile Device Management for Security. Retrieved October 11, 2020, from https://www.identitymanagementinstitute.org/using-mobile-device-management-for-security/.

[35] Mark Pegrum, Grace Oakley, Robert Faulkner. (2013). Schools going mobile: A Study of the Adoption of Mobile Handheld Technologies in Western Australian Independent Schools. *Australasian Journal of Educational Technology,* 29(1).

[36] IT Governance. (2019). Cyber Essentials Controls: Secure Configuration. Retrieved from https://www.itgovernance.co.uk/secure-configuration.

[37] Kadimo, K., Kebaetse, M. B., Ketshogileng, D., Seru, L. E., Sebina, K. B., Kovarik, C., & Balotlegi, K. (2018). Bring-your-own-device in Medical Schools and Healthcare Facilities: A Review of the Literature (Preprint). doi:10.2196/preprints.10764.

[38] Karagiannis, D.; Kühn, H. (2002). Metamodelling Platforms. Proceedings of the Third International Conference EC-Web 2002, p.182.

[39] Kokemuller, N. (2016, October 26). The Role of the Organization's Policies. Retrieved from https://smallbusiness.chron.com/role-organizations-policies-68191.html.

[40] Lord, R. The Real Threat of Identity Theft is in Your Medical Records, Not Credit Cards. 15 December 2017. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/#7c7242da1b59.

[41] Mace, J. C., Parkin, S. E., & Moorsel, A. V. A Collaborative Ontology Development Tool for Information Security Managers. (2010, July). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.8616&rep=rep1&type=pdf.

[42] Marshall, S. (2014, March 01). IT Consumerization: A Case Study of BYOD in a Healthcare Setting. Retrieved from https://timreview.ca/article/771.

[43] Maslove, D. M., Rizk, N., & Lowe, H. J. (2011). Computerized Physician Order Entry in the Critical Care Environment: A

Review of Current Literature. *Journal of Intensive Care Medicine*, 26(3), 165-171. Doi:10.1177/0885066610387984.

[44] Meelhuysen, E. (2018). Protection Vs Privacy: The Problem With Mobile Device Management. Retrieved from https://www.theneweconomy.com/technology/protection-vs-privacy-the-problem-with-mobile-device-management.

[45] Miradore. (2016, October 26). Selective Wipe. Retrieved from https://onlinesupport.miradore.com/hc/en-us/articles/201881101-Selective-wipe.

[46] MOF, O. (2002). OMG Meta Object Facility (MOF) Specification v1. 4.

[47] Moyle, E. (2017, August 29). Security Think Tank: No one-size-fits-all Security Solution. Retrieved from https://www.computerweekly.com/opinion/Security-Think-Tank-No-one-size-fits-all-security-solution.

[48] Murray, Alan. (2015). Achieving a Work-Life Balance with BYOD. Wired. Conde Nast, August 7, 2015. https://www.wired.com/insights/2013/06/achieving-a-work-life-balance-with-byod/.

[49] Ndunge, M. P., Gikandi, J., & Kamau, J. W. (2017). BYOD Security Risks and Mitigation Strategies to Facilitate Adoption. Retrieved from http://academicinsights.org/index.php/AJCIS/article/view/22.

[50] NIST Glossary. (2019). Retrieved from https://csrc.nist.gov/glossary/term/authentication.

[51] NIST. (2019). NIST Glossary. Retrieved from https://csrc.nist.gov/glossary/term/blacklisting.

[52] NIST. (2019). NIST Glossary. Retrieved from https://csrc.nist.gov/glossary/term/encryption..

[53] NIST. (2020). HIPAA Security Standards: Administrative Safeguards. Retrieved from Security Standards: Administrative Safeguards.

[54] NIST. (2020). Security Standards: Technical Safeguards. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf.

[55] Positive Technologies. (2019, September 11). Vulnerabilities and Threats in Mobile Applications, 2019. Retrieved October 11, 2020, from https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/.

[56] Rouse, M. (2012, October 29). What is BYOD (bring your own device) - Definition from WhatIs.com. Retrieved October 09, 2020, from https://whatis.techtarget.com/definition/BYOD-bring-your-own-device.

[57] Spok. (n.d.). 10 Facts About BYOD (2018). Retrieved October 09, 2020, from https://www.spok.com/infographic/infographic-byod/.