Design for Scientific RENAISSANCE

JASER

Privacy and Security Concern for Electronic Medical Record Acceptance and Use: State of the Art

[1]O. M. Enaizan, [2]N. H. Alwi, [3]N. J. Zaizi

[1,2,3]Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia

adi_momane@yahoo.com, najwa@usim.edu.my, njuana@usim.edu.my

Article Info

Received: 1/5/2017
Accepted:28/5/ 2017
Published online: 1/6/2017

ISSN 2231-8844

ABSTRACT

Healthcare sector boosts the usage of information technology (IT) in terms of functions and utility. Electronic Medical Record (EMR) is one of the major applications in the field of e-health. Applying EMR system in the real world may improve the quality of health care and reduce medical errors. However, the level of acceptance and usage of EMR systems among healthcare professionals is low due to privacy and security concerns. To increase the use of EMR, it is important for this issue to be addressed. The aim of this paper is to explore the different factors that affect the EMR acceptance and use, and provides recommendations regarding the development of EMR in the context of privacy and security.

Key words: **healthcare professional, privacy, security, ICT, EMR, e-health**

1. Introduction

In today's environment, most organizations are affected by privacy and data protection requirements. However, for healthcare providers, it is crucial to address the attention to personal information that is related to EMR. Given the risks and related requirements, ensuring the privacy of EMR could be one of the huge challenges to health care providers. A study on patient privacy and data security by (Ponemon, 2011) has reported that scarcity of technology is a great threat to the health care providers who are trying to eliminate the privacy risk. The Symantec Internet Security Threat Report (Haley and Wood, 2013) stated that the percentage of unveiling data violation is much higher in the healthcare industry with the disclosures of EMR, which is potentially sensitive in terms of privacy and security.

In order to improve the medical research and its provision, EMR must be introduced and employed among healthcare providers and doctors (Rahim, Ismail, and Samy, 2013). Another perception of EMR usage in healthcare is to share data for further research, medical innovation,

and for the purpose of making significant decisions in regard to medical customization (Li and Qin, 2013). Therefore, it is crucial to ensure the privacy and security of EMR because it contains patients' sensitive information. There is a lack of empirical studies that examine the factors which affect the adoption of EMR among healthcare providers in the context of privacy and security. Therefore, the purpose of this study is to review privacy and security issues in EMR acceptance and use, and propose EMR development guidelines in the context of privacy and security.

2. Review of literature

2.1 **Privacy and security previous studies**

Research in regard to EMR acceptance and its usage are still insufficient. Vathanophas and Pacharapha, (2010) describe EMR characteristics that affect Electronic Medical Records (EMR) acceptance and developed a conceptual framework, which integrate Technology Acceptance Model (TAM) (Vathanophas and Pacharapha, 2010), functionalities, and security/confidentiality. (Boonstra & Broekhuis, 2010) describe the difficulties encountered by doctors in the adoption of EMRs for the purpose of facilitating implants with the best intervention options. The result showed many barriers in EMR implementation such as legal issues, including privacy and security aspects where there are insufficient security standards for EMRs users. This is why it is considered a critical issue for doctors and patients. Moreover, among other barriers in EMR implementation are confidentiality and authorization. (Ismail and Abdullah, 2011) describe EMR systems in general, theories related to technology adoption, issues related to the adoption of EMR and address issues related to certification, security, privacy, and confidentiality. (Lakbala and Dindarloo, 2014) describe the physician's attitude and perceptions of important EMRs functions, anticipated utilization of EMR functions and also issues affecting the EMRs. The most tackled issues in EMR are privacy and security where the study found that 109 (82.0%) of respondents expressed that the use of EMRs will boost security and 107 (80.4%) of respondents expected the impact on privacy, this issue is supported by many prior studies that shown their concerns about privacy and security of patient data, and as an issue to EMRs usage security, privacy and confidentiality issues were expressed by the majority 60 (45.1%) of physicians. (Najaftorkaman, Ghapanchi, Talaei-Khoei, and Ray, 2015) summarizes a comprehensive classification of the factors influencing the user adoption of EMR and states that the privacy, security, confidentiality, integrity and availability are crucial factors in the adoption of an EMR system. (Kuo, Ma, and Alexander, 2014) describes the relationship between patients' worries about their data security and defensive reactions, and investigate the connection between patients' data security concerns and their data protection privacy reactions towards EMRs, based on protection motivation theory. This study suggested that the collection of information, errors in data collection and secondary usage of information are essential variables in affecting patients' data privacy defensive reactions toward EMRs. (Safadi, Chan, Dawes, Roper, and Faraj, 2015) describes the status of EMR open-source in human services and the capability of open-source to

determine part of the difficulties encompass wide requisition of health IT in North America. The study indicates that there are worries about EMR OSCAR (Electronic Medical Record Open Source Clinical Application Resource), specifically its development and security. Hence, the privacy of medical data is a big concern.

Healthcare adopters and doctors are still in great worry about the privacy and security issues of the patients' data being untreated. Moreover, privacy and security issues remain a major barrier to adoption of EMR (Ochieng and Hosoi, 2005). AL-nassar, Abdullah, and Osman, (2009) believes that understanding these barriers and having the right strategy to deal with these issues will ensure the success of EMR implementation.

Security and privacy are factors that play significant role in the acceptance of any healthcare technology (Wilkowska and Ziefle, 2011). Despite the fact that EMRs have many advantages, the present technologies are not sufficiently utilized to understand its maximum capacity while keeping up patients' privacy. There are numerous key imperatives and difficulties in this area, including security and privacy of EMRs, which are still unsolved and need more consideration from the analyst's groups (Bensefia and Zarrad, 2014). Healthcare IT arrangements must include essential parts inside their security framework approaches and methodology authentication, authorization, availability, confidentiality, data integrity, and nonrepudiation. Moreover, the crucial problem of the modern electronic healthcare industry is security and privacy of patients' record and medical information (Andriole, 2014b). The most common issues in health records are authentication, authorization, availability, confidentiality, data integrity, and nonrepudiation. Moreover, there are three models for privacy concern which are CFIP, IUIPC and IPC. The most model applied in the EMR context is CFIP where it focuses on organizational practices and within one organization. Thus, this study focuses on CFIP model.

Bensefia and Zarrad, (2014) describe doctors' perceptions on the use of EMR. Among their findings are: (1) doctors require a trust that the data will be stored safely on the grounds or else it could make lawful issues, (2) doctors argue whether EMRs are a safe store for patients' data and records, and (3) doctors concern that information in the framework might be available to the individuals who are not authorized to access it. The results of improper divulgence of patient data may prompt lawful issues. Moreover, there are some nations in which an absence of clear security directions could help in understanding patient privacy and confidentiality (Simon et al., 2007). Furthermore, doctors who practice EMR thought that paper recording is more secure than the use of EMR and believe that there are more security and confidentiality risks involved with EMRs. This situation highlights that the privacy and security of patients' record are crucial hurdles in the usage of EMR (Simon et al., 2007).

The most common problems encountered by the user of EMR are security, privacy, and confidentiality (Ismail and Abdullah, 2011). Doctors are also concerned that the patients' information stored in the EMR framework might be misused by unapproved persons and this might lead to legal problems since the patient records are considered confidential (Boonstra and Broekhuis, 2010). Loomis, Ries, Saywell Jr, and Thakker, (2002) describes that the physicians are more concern about this issue than the patients themselves. Furthermore, even among the

physicians who do use EMR, most of them believe that paper records are more secure and confidential than EMR system. This demonstrates how concerns about privacy and security considered as an issue to EMR acceptance. Moreover, without privacy assurances, patients may face problems of whether they should disclose information to health care providers to enhance health care or withhold information to avoid inappropriate use (McGraw, Dempsey, Harris, and Goldman, 2009). Research in (Ismail and Abdullah, 2011) indicate that privacy and security issues in health information system need to be studied in future work. Research in (Najaftorkaman et al., 2015) focuses more on privacy and security issues, including confidentiality, integrity, and availability, which are considered the major concerns in EMR adoption. (Hsieh, 2014) describes the physician acceptance behavior and found that the trust factor affects EMR acceptance. According to Ferreira, Cruz-Correia, Chadwick, and Antunes, (2008) access controls are likely to increase the barrier to acceptance, since their design and implementation are very complex, and their purpose is to deny access to unauthorized people, thus the access control effect on EMR acceptance. (Smith, Milberg, and Burke, 1996) created and approved an instrument that recognizes and measures the essential measurements of individuals' data privacy concerns. The outcomes were a parsimonious 15-item instrument that contains four dimensions of the Concern for Information Privacy (CFIP) scale: collection, secondary use, unauthorized access, secondary use, and errors. The results of these instruments propose that individuals with high privacy concerns, when their information is collected, this information could be miss use for other purposes, the data may be accessed by unauthorized persons, the data are not appropriately handled, and most of the data are inaccurate (Smith et al., 1996). Stewart and Segars, (2002) further verified these four dimensions. Thus, the four dimensions identified by (Smith et al., 1996) appear to provide a complete framework for information privacy concerns and have been mostly cited in previous studies (Zorotheos and Kafeza, 2009; Zhou, 2011). Based on the previous research, many privacy and security issues have to be resolved [26]. This demonstrates that there are limited empirical studies which examined privacy and security factors in EMR context.

2.2 **Method**

a. Resources Searched

Three databases were used to search keywords related to EMR adoption: Science Direct, PubMed, and IEEE Explore.

b. Search Terms

There are three main categories of search terms. The first category focuses on EMR concepts, the second category emphasizes acceptance terms and the last category concentrates on privacy and security. Table 1 shows the three categories of search terms that were used in this study.

Table 1: Three categories of search terms

First category	Electronic Medical Record
Second category	Acceptance, Adoption, Use
third category	Privacy and Security issues

2.3 **Privacy concern**

According to Smith et al., (1996) information privacy concern comprises of four dimensions and it is a multidimensional construct. Collection concerns revolve around people's recognitions regarding whether the information is gathered and kept properly. Secondary use refers to people's worries in regards to whether the information that is gathered for one reason might be improperly utilized for some other reason without approval. Disgraceful access relates to worries about whether unapproved people can see the information. Deceitful access pertains to concerns over whether unauthorized individuals are able to view data. (Smith et al., 1996). There are a number of emerging studies on information privacy study in other disciplines, and introduce numerous dimensions of privacy concerns (Ferreira et al., 2008). Among these measures, there is a high degree of overlap in terms of dimensions measured. However, the most points are commonly discussed in the existing literature are: collection, unauthorized secondary usage, and improper access errors (Hong and Thong, 2013). Every measurement is now delineated as far as its importance in healthcare security. It is perceived that in the near future aggressiveness for the privacy of personal information will be increased as the more information is digitized. The construct CFIP has been used in a limited fashion in IS research and, as yet, has not been widely tested in other disciplines. CFIP model includes: (1) collection data (2) Secondary use (3) Unauthorized access (4) Errors.

a. Collection

Smith et al., (1996) argue that individuals are worried about a large amount of personal information collected and stored by EMRs. Numerous studies use information collection as one of the four points of information privacy concerns (Stone, Gueutal, Gardner, and McClure, 1983). Additionally, (Stewart and Segars, 2002) mentioned that the individual privacy concern relates to the methods of information collection. The simplicity of data collection, data storing, and data transmission of information over electronic systems additionally makes noteworthy dangers to privacy (Gostin et al., 1993).

b. Secondary use

Secondary usage refers to the practice in which information collected for one purpose is

used for other purposes without any legal permission (Milberg, Smith, and Burke, 2000). Furthermore, when the information is not limited to the core objective, the privacy concerns are deteriorated (Sheehan and Hoy, 2000). Thus, individuals concern for information privacy increased when organizations use information elsewhere than the use of it for the reason it was collected (Nowak and Phelps, 1995). According to (Milberg et al., 2000) the usage of personal information even if it is collected and controlled by one organization will generate negative consequences. The definition of a secondary usage for the current study is that the unauthorized usage of individual's health information for any other secondary usage limits the usage of such information to the objective for which it was collected (Smith et al., 1996).

c. Unauthorized access

The key objective to introduce the EMRs in the healthcare is the easy access and sharing of medical data among authorized users like doctors, authorized individuals, and medical staff (Barrows and Clayton, 1996). A mix of an individual's data from different databases makes electronic healthcare data progressively important, but along these lines requires immaculate security from unapproved access (Donaldson and Lohr, 1994). According to (Smith et al., 1996) unauthorized access alludes to individuals' worry that information about them are promptly accessible to individuals not legitimately approved to view or work with this information. According to (Barrows and Clayton, 1996) thirty-three percent of medical professionals demonstrated patient's record is mostly released for unauthorized people in the healthcare sector. In spite of the fact that there is a general presumption that individual should have a "need to know" before they are permitted to access personal information, there is likelihood of dangers to the privacy of data held in medical offices from insiders who may increase unauthorized access to information through specialized technical or other different means (Smith et al., 1996).

d. Errors

According to Smith et al., (1996) errors alludes to the planned and unplanned errors in health data of patients while gathering and storing the data, and then it is considered that the patients do not need to worry about these errors. Individuals may realize that the data about them are being collected, however, they may have worried that the associations involved in the whole procedure are not finding a way to diminish issues that add to errors in individual information (Sheehan and Hoy, 2000). Albeit a few mistakes might be intentional, most privacy-related concerns start from incidental errors in individual information (Milberg et al., 2000).

According to Rothstein, (2007) most of data in the healthcare industry are full with errors, omissions, and this seems normal in this industry. Additionally, in the healthcare industry occurrence of errors is common both in paper recording and electronic recording of data. Hypothetically, electronic patient information can be accepted substantial since medical data frameworks have experienced different quality confirmation methodology, for example, programming, testing, and checking (Terry and Francis, 2007). Furthermore, the errors caused by

human being or due to untrusted electronic system lead to repeated malfunctioning. While most errors have minimal potential of damage, some produce potential harm; subsequently, the aggregate after effects of errors in healthcare industry might be a colossal (Bates et al., 2001).

2.4 **SECURITY CONCERNS IN EMR**

a. Authentication

Authentication is the process of verifying the identity of a user by using a computer system and can be accomplished using log-ins/usernames and passwords, digital certificates, smartcards, and biometrics. Authentication only verifies the identity of an individual; it does not define their access (authorization) (Andriole, 2014a). To ensure that the clients and other documents are original and they have not been created is necessary for authenticity. The originality of data and documents are essential for computing. Lhotska, Prague, and Aubrecht, (2008) also argue that to maintain authenticity it is important that both parties must provide their original identity, they mention in the online or in any other data record.

b. Confidentiality

According to Pappas, (2008) confidential information can only be provided to the users who are authorized to access, use, and copy the information only if they need information for any productive purpose. When confidential information have been accessed, used, and copied for unauthorized persons, then there will be a confidential breach (Alanazi, Alam, Zaidan, and Zaidan, 2010). For instance, allowing an individual to look behind you at your system screen that contains private information would be a break of secrecy for the reason of authorization and privacy concerns. In addition, giving private information through the telephone to unauthorized individuals is considered as a breach of confidentiality (Sattarova Feruza and Kim, 2007). Confidentiality of data refers to the process in which data is secured from the access of unauthorized persons (Taute, 2009). In other words, confidentiality means that necessary cautions that are taken to secure data from the access of unauthorized systems and persons and limit the access of data only to the authorized persons and to those who are really in need to use the information. At the point when organizations endeavor to increase secret data about another organization, it is most often for monetary benefits. These organizations can utilize the data to offer or exchange an item with the end goal of bringing themselves into that part of the business sector. Pouloudi, (1999) describes that most of the businesses do that to break the monopoly of other organizations by offering the same product in the market and gain some share of the market. (Gellman, 2002) has reported that 92% of the households do not trust online businesses to collect their confidential information.

c. Integrity

Integrity refers to the modification of data without the permission of authorized individuals (Sattarova Feruza and Kim, 2007). This is certainly different from referential integrity in databases. Integrity (Aich, 2009) is disregarded when a worker accidentally or on purpose erases critical information, a virus corrupts a computer system or when an employee adjusts his own compensation in a finance database, when an unauthorized client vandalizes a site, and somebody can cast the countless votes in an online survey, and so on. A number of ways exist that can violate the integrity without any malevolent intention (Sattarova Feruza and Kim, 2007). In the least complex case, a client on a framework could miss-sort somebody's location. On a bigger level, if a computerized procedure is not composed and tried accurately, high-level of redesigns to a database could adjust information in an off base way, leaving the integrity of the information compromised. The information security experts are striving control the data integrity errors (Alanazi et al., 2010).

d. Availability

According to the Sattarova Feruza and Kim, (2007) availability implies that the data, the electronic system used to collect the data and the security controls used to ensure that the data is accessible and working accurately when the data is required. Any information system can only fulfill its purpose of using when it is able to deliver information when it is needed (Sattarova Feruza and Kim, 2007). In other words, the electronic data collection systems, tools to maintain the security and privacy of data, other communication systems must be working properly (Hwang and Syamsuddin, 2009). Systems that offer high availability ensure the availability of data every time, even if there is a problem of hardware failure, preventing service disruptions due to power outages (Zhang and Liu, 2010).

e. Non-repudiation

Non-repudiation ensures that transferred data are sent and received by the parties to provide a record of the transaction. Digital signatures and system audit logs of all user activity are methods of non-repudiation. Moreover, non-repudiation ensures that a party cannot refute the validity of a statement or contract and that a transferred data has been sent and received by the parties claiming to have sent and received the data; methods of ensuring such include digital signature, the use of public and private keys, and auditing of all user activity (Andriole, 2014a).

2.5 **CONCLUSION**

This study has reviewed the privacy and security concerns of EMR acceptance and usage. It also reviewed other related work to demonstrate the gap in previous studies, as EMR acceptance, lack to many privacy and security issues. The privacy and security factors play an important role in increasing the level of acceptance, thus, these issues are treated in this regard, such as confidentiality, integrity, availability, trust and CFIP model. This study concludes that authentication, confidentiality, data integrity, non-repudiation, availability, data collection, secondary usage, unauthorized access and errors are the most concerned factors to healthcare professionals. These factors are crucial as a guideline in an EMR development in the context of privacy and security. For future work it is significant to develop a framework for privacy and security issues in EMR acceptance and usage among health care professionals and test the framework.

References

Aich, D. (2009). Secure query processing by blocking sql injection. National Institute of Technology Rourkela.

AL-nassar, B. A. Y., Abdullah, M. S., & Osman, W. R. S. (2009). Barriers for implementation of electronic medical record (EMR). In Proc. 4th International Conference on Information Technology.

Alanazi, H. O., Alam, G. M., Zaidan, B. B., & Zaidan, A. A. (2010). Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. Journal of Medicinal Plants Research, 4(19), 2059–2074.

Andriole, K. P. (2014a). Security of electronic medical information and patient privacy: what you need to know. Journal of the American College of Radiology, 11(12), 1212–1216.

Andriole, K. P. (2014b). Security of electronic medical information and patient privacy: What you need to know. Journal of the American College of Radiology, 11(12), 1212–1216. https://doi.org/10.1016/j.jacr.2014.09.011

Barrows, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. Journal of the American Medical Informatics Association, 3(2), 139–148.

Bates, D. W., Cohen, M., Leape, L. L., Overhage, J. M., Shabot, M. M., & Sheridan, T. (2001). Reducing the frequency of errors in medicine using information technology. Journal of the American Medical Informatics Association, 8(4), 299–308.

Bensefia, A., & Zarrad, A. (2014). A Proposed Layered Architecture to Maintain Privacy Issues in Electronic Medical Records. E-Health Telecommunication Systems and Networks, 3(4), 43.

Boonstra, A., & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. BMC Health Services Research, 10(1), 1.

Donaldson, M. S., & Lohr, K. N. (1994). Health data in the information age: use, disclosure, and privacy. National Academies Press.

Ferreira, A., Cruz-Correia, R., Chadwick, D., & Antunes, L. (2008). Improving the implementation of access control in EMR. In Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on (pp. 47–50). IEEE.

Gellman, R. (2002). Privacy, Consumers, and Costs.

Gostin, L. O., Turek-Brezina, J., Powers, M., Kozloff, R., Faden, R., & Steinauer, D. D. (1993). Privacy and security of personal information in a new health care system. JAMA, 270(20), 2487–2493.

Haley, K., & Wood, P. (2013). 2013 Internet security threat report. Mountain View: Symantec Corporation.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. MIS Quarterly, 37(1), 275–298.

Hsieh, P.-J. (2014). Physicians' acceptance of electronic medical records exchange: An extension of the decomposed TPB model with institutional trust and perceived risk. International Journal of Medical Informatics, (June), 1–14. https://doi.org/10.1016/j.ijmedinf.2014.08.008

Hwang, J., & Syamsuddin, I. (2009). Information Security Policy Decision Making: An Analytic Hierarchy Process Approach. In 2009 Third Asia International Conference on Modelling & Simulation (pp. 158–163). IEEE.

Ismail, N. I. B., & Abdullah, N. H. B. (2011). Developing electronic medical records (EMR) framework for Malaysia's public hospitals. In Humanities, Science and Engineering (CHUSER), 2011 IEEE Colloquium on (pp. 131–136). IEEE.

Kuo, K.-M., Ma, C.-C., & Alexander, J. W. (2014). How do patients respond to violation of their information privacy? Health Information Management Journal, 43(2), 23–33.

Lakbala, P., & Dindarloo, K. (2014). Physicians' perception and attitude toward electronic medical record. Springerplus, 3(1), 1.

Lhotska, L., Prague, C., & Aubrecht, P. (2008). Deliverable D09 Security of the Multi Agent System. Agent System.

Li, X.-B., & Qin, J. (2013). A Framework for Privacy-Preserving Medical Document Sharing.

Loomis, G. A., Ries, J. S., Saywell Jr, R. M., & Thakker, N. R. (2002). If electronic medical records are so great, why aren't family physicians using them?(Original Research). Journal of Family Practice, 51(7), 636–642.

McGraw, D., Dempsey, J. X., Harris, L., & Goldman, J. (2009). Privacy as an enabler, not an impediment: building trust into health information exchange. Health Affairs, 28(2), 416–427.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. Organization Science, 11(1), 35–57.

Najaftorkaman, M., Ghapanchi, A. H., Talaei- Khoei, A., & Ray, P. (2015). A taxonomy of antecedents to user adoption of health information systems: A synthesis of thirty years of research. Journal of the Association for Information Science and Technology, 66(3), 576–598.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual- level consumer information: Determining how and when "privacy" matters. Journal of Direct Marketing, 9(3), 46–60.

Ochieng, O. G., & Hosoi, R. (2005). Factors influencing diffusion of electronic medical records: a case study in three healthcare institutions in Japan. Health Information Management, 34(4), 120–129.

Pappas, J. A. (2008). A revitalized information assurance training approach and information assurance best practice rule set. Monterey, California. Naval Postgraduate School.

Ponemon, I. R. R. (2011). Benchmark study on patient privacy and data security. Journal of Healthcare Protection Management: Publication of the International Association for Hospital Security, 27(1), 69.

Pouloudi, A. (1999). Information technology for collaborative advantage in healthcare revisited. Information & Management, 35(6), 345–356.

Rahim, F. A., Ismail, Z., & Samy, G. N. (2013). Information privacy concerns in electronic healthcare records: A systematic literature review. In 2013 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 504–509). IEEE.

Rothstein∗ , M. A. (2007). Health privacy in the electronic age. The Journal of Legal Medicine, 28(4), 487–501.

Safadi, H., Chan, D., Dawes, M., Roper, M., & Faraj, S. (2015). Open-source health information technology: A case study of electronic medical records. Health Policy and Technology, 4(1), 14–28.

Sattarova Feruza, Y., & Kim, T. (2007). IT security review: Privacy, protection, access control, assurance and system security. International Journal of Multimedia and Ubiquitous Engineering, 2(2), 17–32.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. Journal of Public Policy & Marketing, 19(1), 62–73.

Simon, S. R., Kaushal, R., Cleary, P. D., Jenter, C. A., Volk, L. A., Orav, E. J., … Bates, D. W. (2007). Physicians and electronic health records: a statewide survey. Archives of Internal Medicine, 167(5), 507–512.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly, 167–196.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. Information Systems Research, 13(1), 36–49.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology, 68(3), 459.

Taute, B. (2009). DST-funded information security centre of competence.

Terry, N. P., & Francis, L. P. (2007). Ensuring the privacy and confidentiality of electronic health records. University of Illinois Law Review, (2), 681–736. https://doi.org/10.1215/03616878-27-6-1046

Vathanophas, V., & Pacharapha, T. (2010). Information technology acceptance in healthcare service: The study of electronic medical record (EMR) in Thailand. In PICMET 2010 TECHNOLOGY MANAGEMENT FOR GLOBAL ECONOMIC GROWTH (pp. 1–5). IEEE.

Wilkowska, W., & Ziefle, M. (2011). Perception of privacy and security for acceptance of E-health technologies: Exploratory analysis for diverse user groups. In 2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops (pp. 593–600). IEEE.

Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. In 2010 IEEE 3rd International Conference on Cloud Computing (pp. 268–275). IEEE.

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. Industrial Management & Data Systems, 111(2), 212–226.

Zorotheos, A., & Kafeza, E. (2009). Users' perceptions on privacy and their intention to transact online: a study on Greek internet users. Direct Marketing: An International Journal, 3(2), 139–153.