Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 138 (2018) 12–19

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN/HCist 2018

Security aspects in healthcare information systems: A systematic mapping

Aqsa Fatima, Ricardo Colomo-Palacios*

Østfold University College, B R A Veien 4, Halden 1783, Norway

Abstract

The security of patient's data is the most overbearing barrier to access when considering the adoption of Healthcare Information Systems (HIS) in the healthcare industry. Recently, several studies were conducted to address security risks, and a series of solutions were proposed to enable data and privacy protection. In this paper we conduct the systematic mapping review to know more about security aspects in HIS. Our study provides a comprehensive review of the literature on the evaluation and implementation of HIS security, detailing the challenges and recommendations for implementers and adopters alike. The purpose of this paper is to analyse the security perspective and some of the important concerns that need to be considered to successfully use information systems in healthcare.

Keywords: Healthcare Information systems; Data security;Cloud computing; Guidelines;Measures; Threats

*Corresponding author. Tel.: + 47 6921 5000; fax: + 47 6921 5002.
E-mail address: ricardo.colomo-palacios@hiof.no

10.1016/j.procs.2018.10.003

1. Introduction

Security is an important aspect of all information processing activities, mainly in those environments where information is presenting critical and confidential nature, as in the case of healthcare settings[1]. It has been claimed that Health Information systems (HIS) can offer economic benefits through efficiency, data management and administration of care. HIS can become more beneficial when health information shared between patients and their healthcare providers are used to improve the diagnosis, increase patient education and promote self-care[2]. The idea of computerized patient records was introduced in the 1960s and 1970s, and many attempts have been made with various degrees of success and failures[3]. In recent years, HIS has emerged as a patient-centric model of health information exchange. In such settings, cloud computing infrastructure is able to reduce the cost of hardware resources and energy consumption, with less data center space and provide flexibility when changing software components[4][5]. Cloud computing improves the level of healthcare services enables collaboration and communication between the different actors (health professionals, patients, administrators, developers) in the health care field[6]. When cloud resources and services are open for public use, it is referred to as an untrusted cloud environment e.g., Amazon AWS, Microsoft Azure, and Google are the cloud platform and not fully trusted by users [7]. In terms of security, cloud computing cannot be handle with a single method, we require many traditional, new technologies and strategies altogether[8]. IT people have adopted IT tools such as encryption, firewalls, access management, and backup systems to deal with the security issues in HIS [9].According to the Michael Nadeau(CSO editor), in 2018 HIS continues to be a popular target for ransomware, crypto mining, data theft, phishing, and insider threats[10]. The patient privacy is protected under the public law 104-191 that, also known as the Health Insurance Portability and Accountability Act (HIPAA)[11]. In HIPAA, two key requirements are privacy and security regulations and violations of these, not only may cause the disclosure of patients' sensitive information, but also can bring great economic loss and reputation damage to healthcare providers[12][13]. In an environment in which security is key for all information systems and, on the other hand, security aspects seem key for HIS, we need to further study how HIS security is affecting the whole field. The objective of this paper is to structure and characterize the state of the practice on HIS security. In consequence, the authors of this study conducted a systematic mapping review to identify, select, classify and analyze primary studies published in scientific outlets. To the best of our knowledge, no systematic mapping review on HIS security has been published yet. The remainder of this paper proceeds as follows. Section 2 describes the method followed in this research work. Section 3 analyses and discusses the results of the systematic mapping review. Section 4 wraps up the paper and presents main conclusions on the study.

2. Systematic Mapping

The study follows the guidelines provided by Petersen et al. [14]. Figure 1 details the process adopted.

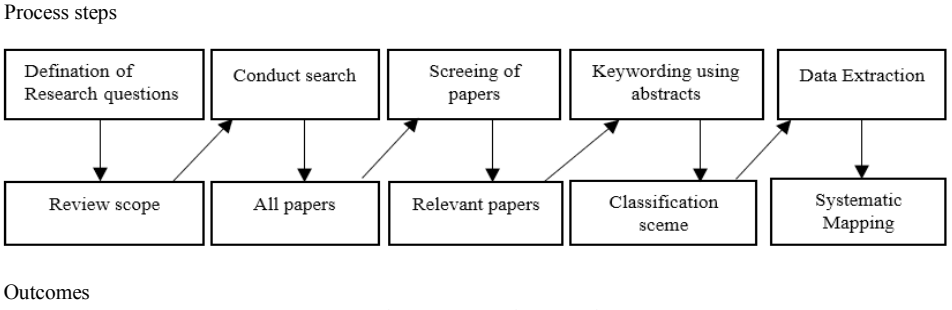

Fig. 1. Systematic Map Diagram

The essential process steps of our systematic mapping study are definition of research questions, conducting the search for relevant papers, screening of papers, keywording of abstracts and data extraction and mapping (Fig. 1). Each process steps have an outcome, the final outcome of the process being the systematic map.

2.1. Research scope and Research questions

The main goal of our systematic mapping study is to provide an overview of the research area and type of research and results available within it. A secondary goal is to identify the forums in which research in the area has been published. Thus, the main research question driving this study is:

What is the state of the practice of security aspects in HIS?

After presenting main research question, this leads us to divide it in a set of sub questions as follows:

RQ1: What are the most reported deployment methods in HIS?
RQ2: What are the most cited guidelines/rules and regulations for data security in HIS?
RQ3: What are the most reported security incidents/threats in HIS?
RQ4: What are the most reported security measures in HIS?

In RQ1, we focus on deployment approaches related to HIS. In RQ2 we are interested in getting more detail about rules and regulations that are in sighted in terms of HIS security. To answer RQ3 and RQ4 we need to know: first, what types of threats are faced by HIS, then we follow the mechanism against them.

2.2. Search strategy

As a research method, systematic mapping was adopted due to its adequacy for the exploration of a research area in a systematic way. In this step, it is important to identify the search strategy adopted. In our procedure the following digital libraries were used: Wiley Online Library, IEEE Digital Library, ScienceDirect, Springer, ACM Digital Library and Google Scholar. These libraries were used because of their popularity in the broad computing field. Table 1 presents papers retrieved and filtered in libraries analysed.

Table 1. Papers distribution

Source	Initial Results	Final Studies
Wiley Online Library	12	5
IEEE Digital Library	104	39
Elsevier (ScienceDirect)	28	13
Springer	20	7
ACM Digital Library	12	4
Google Scholar	25	17
Total	***201***	***85***

Regarding the keywords for the search, after some exploratory searches using different combination of keywords, the researchers jointly established the final string to be used in the search:
"Healthcare information system": (data security OR threats OR guidelines OR measures OR cloud computing)

2.3. Study Selection: Inclusion & exclusion criteria

Inclusion and exclusion criteria are used to exclude studies that are not relevant to answer the research questions. We found it useful to exclude papers which only mentioned our main focus, variability, in introductory sentences in the abstract. This was needed since it is a central concept in the area and thus is frequently used in abstracts without papers really addressing it any further. Our inclusion and exclusion criteria are shown in Table 2.

Table 2. Inclusion and exclusion criteria

Inclusion
(1) Keynotes, conference papers, journal papers dealing with Healthcare Information System.
Exclusion
(1) The abstract made obvious that a contribution lies outside the Healthcare Information system.
(2) The content of the paper showed that the term "Healthcare Information System" has been used only occasionally. We only checked this if the term "Healthcare Information System" is not explicitly mentioned in title or abstract.
(3) The contribution was only available in the form of abstracts or PowerPoint presentations.
(4) Type of publication could not be determined (technical report, conference, journal, keynote)
(5) Publication language was not English.

(6) Papers published before 2010

2.4. Study classification

For our study, we followed a systematic process shown in Fig. 2 based on [13]. Here we use Keywording for to reduce the time needed in developing the classification scheme and ensuring that the scheme takes the existing studies into account. Keywording is done in two steps. First, we read abstracts and look for keywords and concepts that reflect the contribution of the paper. While doing so, we also identified the context of the research. This helps us to come up with a set of categories which is representative of the underlying population. When abstracts are of too poor quality to allow meaningful keywords to be chosen, then we also study the introduction or conclusion sections of the paper. When a final set of keywords was chosen, then we clustered it and used to form the categories for the map.

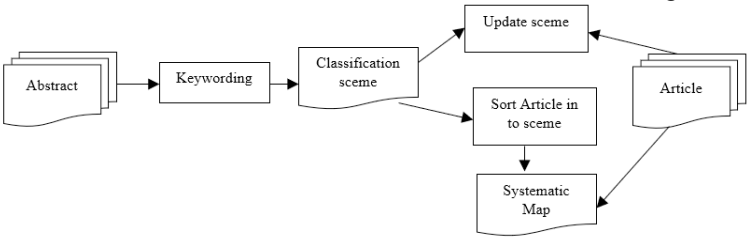

Fig. 2. Classification Scheme

In our study, three main aspects were analysed. Firstly, deployment methods, rules and regulations, threats and measures. Secondly, the type of contribution was considered, which for example could be a process, method, framework etc. shown in Table 3 and lastly, the kind of research developed (shown in Table 4).

KIND OF CONTRIBUTION

Authors adopted the approach by Ruiz-Rube et al [15] and the final classification is as follows:

Table 3. Contribution type

Category	Description
Process	Contemplates those works whose contribution is described by the authors in terms of HIS, method content, methodologies, or guidelines.
Model	Covers those papers that contribute to the field with an extension to the HIS model or with a new one based on it or clearly defined in paper.
Tool	Is used for those papers that present a standalone application or an extension of some other one.
Framework	Here, we consider those works that contribute with a combination of the previous three elements or clearly defined in paper (i.e., with a process, a model, and a tool).
Mapping	Under this type of contribution, we group those works that describe a transformation process between models or indicate a mapping between elements of different models.
Technique	A procedure used to accomplish a specific activity or task. It could come accompanied with a support tool.

RESEARCH TYPE

This refers to the research approach followed by the authors in the paper. We adopted the approach proposed by Petersen et al. [13]. This classification identifies the following categories:

Table 4. Research type

Category	Description
Solution proposal	A solution for a problem is proposed, the solution can be either novel or a significant extension of an existing technique. The potential benefits and the applicability of the solution is shown by a small example or a good line of argumentation
Evaluation papers	Techniques are implemented in practice and an evaluation of the technique is conducted. That means, it is shown how the technique is implemented in practice (solution implementation) and what are the consequences of the implementation in terms of benefits and drawbacks (implementation evaluation).
Validation Research	Techniques investigated are novel and have not yet been implemented in practice. Techniques used are for example experiments, i.e., work done in the lab.

Philosophical Papers	These papers sketch a new way of looking at existing things by structuring the field in form of a taxonomy or conceptual framework.
Opinion Papers	These papers express the personal opinion of somebody whether a certain technique is good or bad, or how things should be done. They do not rely on related work and research methodologies.
Experience Papers	Experience papers explain on what and how something has been done in practice. It has to be the personal experience of the author.

These schemes allow to classify non-empirical research in the categories solution proposal, opinion papers, experience papers, philosophical papers, evaluations paper and validation research.

2.5. Data extraction and mapping of results

When having the classification scheme in place, the relevant articles were sorted into the scheme, i.e., the actual data extraction took place. As shown in Fig. 2, the classification scheme evolves while doing the data extraction, like adding new categories or merging and splitting existing categories. In this step, we used an Excel sheet to document the data extraction process. Table 3 and Table 4 present each category of the classification scheme. The analysis of the results focuses on presenting the frequencies of publications for each category. This makes it possible to see which categories have been emphasized in past research and thus to identify gaps and possibilities for future research. In our study, we used a bubble plot to report the frequencies, shown in Fig. 3. This is basically two x-y scatterplots with bubbles in category intersections. The size of a bubble is proportional to the number of articles that are in the pair of categories corresponding to the bubble coordinates. In this diagram, we can see that the most frequent type of study contribution is the definition of processes and, to a lesser degree, models. From the point of view of the research type, most of the primary studies are evaluation papers, followed by solution proposal.

Fig. 3. Systematic Map by means of a bubble plot

3. Analysis and Discussion

The discussion below deals in order with each of the research question. The themes in the articles were examined by means of content analysis. Each section begins with a description of the criteria informing the analysis. This is followed by a presentation of the results, which are finally summarized in Excel document.

RQ1: What are the most reported deployment methods in HIS?

Our study discovered that the major research efforts focus on the deployment of cloud computing in terms of cost and accessibility of data. According to [16], healthcare professionals are becoming hard to find, also costs of healthcare services rise with every passing day. The significance of adopting cloud computing paradigm in the healthcare sector are flexibility, cost effectivity and high-performance, authors also presented a different models for ensuring cloud computing security[17][18]. However, many healthcare organizations are still reluctant to adapt cloud computing due

to security shortcoming associated with its infrastructure and to sensitive patient data [19].
The three most common deployment models are 1) Private Cloud 2) Public Cloud 3) Hybrid Cloud [20]. Authors also support the multi-cloud Infrastructure instead single cloud and report, according to their experience, that single-cloud is far more vulnerable to failure of service unavailability and malicious insiders and due to this reason, it is less popular in healthcare, as HIS are concerned about its security[21].
For Cloud computing, the US National Institute of Standards and Technology (NIST) listed 3 services 1) Software as a service (SaaS) 2) Platform as a service (PaaS) 3) Infrastructure as a service (IaaS) as presented in [22][23]. To conclude the answer to this research question, studies those considering the strategic value of implementing cloud computing in healthcare industry, suggest the Balanced Scorecard Approach (BSA)[24]. Others propose cloud computing as a new business paradigm for biomedical information sharing[25].
RQ2: What are the most cited guidelines/rules and regulations for data security in HIS?

According to our study, many health care providers follow the HIPAA security and privacy rule. They establish a standard for the protection of health information either that is transferred in electronic form or related to privacy of i*ndividually identifiable* information and HIPAA is a federal security law that sets a baseline of protection for certain individually identifiable health [26,27]. Additionally, in [28] authors perform a comparison between HIPAA and ISO, and purpose of conforming the ISO standards to determine whether the existing protocol could be well fitted to achieve HIPAA compliance. Our study discovered that, there are total 2 guidelines for HIS security 1) HIPAA 2)ISO 27799:2016[28].
RQ3: What are the most reported security incidents/threats in HIS?
Cybercriminals always try to discover new ways to beat the most sensitive networks, so protection of healthcare data is a growing challenge, but awareness is the first step[29].
Our study discovered that there are altogether 18 types of major and minor threats to HIS. Table 5 presents these threats with a description for each. Basically, the threats were categorized based on a comparative study of previous works and publications[30][31][32][33][34]as well as on the study conducted in this research.

Table 5. HIS Threats

Threat	Description
Electronic / Internet of Things (IOT) devices	• Hackers • Security breaches • Power breakdown
Inside threat(staff)	• Stealing the data • Misuse of password • Discard equipment without removed the information • Accidently misuse data (transfer to wrong person, delete or modified). • Lack of system usage, training of staff
Third-party Entry Software	Vendors (software and hardware) • Outdated antivirus • System bugs
Network	• Lack of Encryption • Neglecting proper security Configuration • Security alert, software outdated • Network breakdown
Natural hazards	• Floods • Fire • Cyclone

As per our study, staff is a serious threat to the confidentiality, integrity, and availability of data. According to [30], incidents happen due to lack of awareness and good practice among the staff.
To conclude this section, we know that accurate, up-to-date and quality information is necessary in healthcare discipline. From study we conducted, we found that the two most common privilege negligence are 1) transfer password to other persons 2) use one password for all purposes.
RQ4: What are the most reported security measures in HIS?

In the healthcare sector, the misconception of security is one of the key problems in the adoption of cloud as a de facto standard [20]. In this research, we found that there is a panoply of privacy and security frameworks that are already in presence, only we need to take leverage from the existing process and utilize these standards in the field of

healthcare[35]. These proposed frameworks respond in multiple ways like, prevent untrusted applications from reading files that are owned by healthcare organization and also prevent storage of sensitive information on the file system[36]. Although technical safeguards are essential to the security of HIS, good training, awareness programs and adopting a proper information security policy are particularly important to prevent insiders from causing security incidents[33]. Our study discovered 9 technical solutions for HIS. Table 6 presents these technical solutions with a description for each. Basically, these measures were identified with previous works and publications[33][37][38] as well as on the case study conducted in this research.

Table 6. HIS Measures

Measure	Description
Access control	• Employ a strong authentication mechanism • Use software, for reminder to change password after one year • Availability of services, only authorized user and don't pass password to others.
Secure use of the Internet	• Block web pages
Secure data storage on external media	• Disable or limit the use of portable storage devices • Encrypt data stored on removable memory devices
Secure use of e-mail	• Encrypt all messages • Use password-protected screen savers • Security alert, software outdated

Moreover, malware is another threat. Malware gathers sensitive information or spread position in a silent way [39]. Some authors devote their work to detect malware[40] [39].To conclude this section, authors found that insider attacks are becoming increasingly detrimental and frequent, affecting critical infrastructure at a massive scale [41]. According to our research, two easy steps reduce the security incidents are 1) proper staff training 2) implement proper healthcare guidelines and procedures for to achieving a high level of information assurance in healthcare systems and also need to implement an appropriate security controls at all levels of HIS architecture to ensure data protection from both internal and external threats[42].

4. Limitations and Conclusions

HIS security is considered one of the most important fields for healthcare industry. However, and despite of its importance, HIS implementation and exploitation are still challenging. The challenges we identified should not be seen as deterrents to implementing HIS security. As cloud computing implementation, better methods, practices, tools etc. can probably overcome them. The benefits we identified (efficiency, promote self-care and data management) will also boost HIS. However, it is also true that technical safeguards are highly important for HIS security. However, we notice that training and awareness are the best non-technical safeguards to overcome the insiders' security and privacy threats.

References

[1] Stahl Bernd Carsten, Doherty Neil F., Shaw Mark. Information security policies in the UK healthcare sector: a critical evaluation. Inf Syst J 2011;22:77–94. doi:10.1111/j.1365-2575.2011.00378.x.
[2] Paul RJ, Ezz I, Kuljis J. Healthcare information systems: a patient-user perspective. Health Syst 2012;1:85–95. doi:10.1057/hs.2012.17.
[3] Boulus N, Bjorn P. A cross-case analysis of technology-in-use practices: EPR-adaptation in Canada and Norway. Int J Med Inf 2010;79:e97–108. doi:10.1016/j.ijmedinf.2008.06.008.
[4] Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Trans Parallel Distrib Syst 2013;24:131–43. doi:10.1109/TPDS.2012.97.
[5] Chioreanu RC, Crişan-Vida M, Stoicu-Tivadar L, Stoicu-Tivadar V. Implementing and securing a hybrid cloud for a healthcare information system. 2014 11th Int. Symp. Electron. Telecommun. ISETC, 2014, p. 1–4. doi:10.1109/ISETC.2014.7010776.
[6] Ouardi A, Sekkaki A, Mammass D. Towards an inter-Cloud architecture in healthcare system. 2017 Int. Symp. Netw. Comput. Commun. ISNCC, 2017, p. 1–6. doi:10.1109/ISNCC.2017.8071986.
[7] Tang J, Cui Y, Li Q, Ren K, Liu J, Buyya R. Ensuring Security and Privacy Preservation for Cloud Data Services. ACM Comput Surv 2016;49:13:1–13:39. doi:10.1145/2906153.
[8] Liu W. Research on cloud computing security problem and strategy. 2012 2nd Int. Conf. Consum. Electron. Commun. Netw. CECNet, 2012, p. 1216–9. doi:10.1109/CECNet.2012.6202020.
[9] Ferreira A, Antunes L, Chadwick D, Correia R. Grounding information security in healthcare. Int J Med Inf 2010;79:268–83. doi:10.1016/j.ijmedinf.2010.01.009.
[10] Nadeau M. 5 biggest healthcare security threats for 2018. CSO Online 2018. https://www.csoonline.com/article/3262187/healthcare/5-

biggest-healthcare-security-threats-for-2018.html (accessed April 22, 2018).
[11] Alshugran T, Dichter J. Extracting and modeling the privacy requirements from HIPAA for healthcare applications. IEEE Long Isl. Syst. Appl. Technol. LISAT Conf. 2014, 2014, p. 1–5. doi:10.1109/LISAT.2014.6845198.
[12] Huang H-F, Liu K-C. Efficient key management for preserving HIPAA regulations. J Syst Softw 2011;84:113–9. doi:10.1016/j.jss.2010.08.056.
[13] Wu R, Ahn G-J, Hu H. Towards HIPAA-compliant Healthcare Systems. Proc. 2Nd ACM SIGHIT Int. Health Inform. Symp., New York, NY, USA: ACM; 2012, p. 593–602. doi:10.1145/2110363.2110429.
[14] Petersen K, Feldt R, Mujtaba S, Mattsson M. Systematic Mapping Studies in Software Engineering n.d.:11.
[15] Ruiz- Rube Iván, Dodero Juan Manuel, Palomo- Duarte Manuel, Ruiz Mercedes, Gawn David. Uses and applications of Software & Systems Process Engineering Meta- Model process models. A systematic mapping study. J Softw Evol Process 2013;25:999–1025. doi:10.1002/smr.1594.
[16] AbuKhousa E, Mohamed N, Al-Jaroodi J. e-Health Cloud: Opportunities and Challenges. Future Internet 2012;4:621–45. doi:10.3390/fi4030621.
[17] Bamiah M, Brohi S, Chuprat S, Manan J l A. A study on significance of adopting cloud computing paradigm in healthcare sector. 2012 Int. Conf. Cloud Comput. Technol. Appl. Manag. ICCCTAM, 2012, p. 65–8. doi:10.1109/ICCCTAM.2012.6488073.
[18] Setareh S, Rezaee A, Farahmandian V, Hajinazari P, Asosheh A. A cloud-based model for hospital information systems integration. 2014 7th Int. Symp. Telecommun. IST, 2014, p. 695–700. doi:10.1109/ISTEL2014.7000792.
[19] Barthelus L. Adopting cloud computing within the healthcare industry: opportunity or risk? 2016;4:16.
[20] Abrar H, Hussain SJ, Chaudhry J, Saleem K, Orgun MA, Al-Muhtadi J, et al. Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry. IEEE Access 2018;PP:1–1. doi:10.1109/ACCESS.2018.2805919.
[21] Khattak HAK, Abbass H, Naeem A, Saleem K, Iqbal W. Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure. 2015 17th Int. Conf. E-Health Netw. Appl. Serv. Heal., 2015, p. 61–7. doi:10.1109/HealthCom.2015.7454474.
[22] Mell P, Grance T. The NIST Definition of Cloud Computing n.d.:7.
[23] Kuo AM-H. Opportunities and Challenges of Cloud Computing to Improve Health Care Services. J Med Internet Res 2011;13. doi:10.2196/jmir.1867.
[24] Alharbi F, Atkins A, Stanier C, Al-Buti HA. Strategic Value of Cloud Computing in Healthcare Organisations Using the Balanced Scorecard Approach: A Case Study from a Saudi Hospital. Procedia Comput Sci 2016;98:332–9. doi:10.1016/j.procs.2016.09.050.
[25] Rosenthal A, Mork P, Li MH, Stanford J, Koester D, Reynolds P. Cloud computing: A new business paradigm for biomedical information sharing. J Biomed Inform 2010;43:342–53. doi:10.1016/j.jbi.2009.08.014.
[26] Hu J, Chen H-H, Hou T-W. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Comput Stand Interfaces 2010;32:274–80. doi:10.1016/j.csi.2009.04.005.
[27] Mirkovic J, Skipenes E, Christiansen EK, Bryhni H. Security and privacy legislation guidelines for developing personal health records. 2015 Second Int. Conf. EDemocracy EGovernment ICEDEG, 2015, p. 77–84. doi:10.1109/ICEDEG.2015.7114460.
[28] Gardazi SU, Shahid AA, Salimbene C. HIPAA and QMS Based Architectural Requirements to Cope with the OCR Audit Program. 2012 Third FTRA Int. Conf. Mob. Ubiquitous Intell. Comput., 2012, p. 246–53. doi:10.1109/MUSIC.2012.50.
[29] University G. Top 10 Threats to Information Security. GTN SCS 2015. https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology (accessed April 22, 2018).
[30] Samy GN, Ahmad R, Ismail Z. Security threats categories in healthcare information systems. Health Informatics J 2010;16:201–9. doi:10.1177/1460458210377468.
[31] Pankomera R, Greunen D van. Mitigating vulnerabilities and threats for patient-centric healthcare systems in low income developing countries. 2017 IST-Afr. Week Conf. IST-Afr., 2017, p. 1–11. doi:10.23919/ISTAFRICA.2017.8102384.
[32] Luca GD, Brattstrom M, Morreale P. Designing a secure e-health network system. 2016 Annu. IEEE Syst. Conf. SysCon, 2016, p. 1–5. doi:10.1109/SYSCON.2016.7490528.
[33] Fernández-Alemán JL, García ABS, García-Mateos G, Toval A. Technical solutions for mitigating security threats caused by health professionals in clinical settings. 2015 37th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBC, 2015, p. 1389–92. doi:10.1109/EMBC.2015.7318628.
[34] Piliouras T, Yu PL, Su Y, Siddaramaiah VKA, Sultana N, Meyer E, et al. Trust in a cloud-based healthcare environment. 2011 8th Int. Conf. Expo Emerg. Technol. Smarter World, 2011, p. 1–6. doi:10.1109/CEWIT.2011.6135890.
[35] Puppala M, He T, Yu X, Chen S, Ogunti R, Wong STC. Data security and privacy management in healthcare applications and clinical data warehouse environment. 2016 IEEE-EMBS Int. Conf. Biomed. Health Inform. BHI, 2016, p. 5–8. doi:10.1109/BHI.2016.7455821.
[36] Ahmed M, Ahamad M. Protecting Health Information on Mobile Devices. Proc. Second ACM Conf. Data Appl. Secur. Priv., New York, NY, USA: ACM; 2012, p. 229–240. doi:10.1145/2133601.2133629.
[37] Mhatre S, Nimkar AV, Dhage SN. Comparative study on attribute-based encryption for health records in cloud storage. 2017 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT, 2017, p. 647–52. doi:10.1109/RTEICT.2017.8256677.
[38] Harvey Melissa J., Harvey Michael G. Privacy and security issues for mobile health platforms. J Assoc Inf Sci Technol 2014;65:1305–18. doi:10.1002/asi.23066.
[39] Souri A, Hosseini R. A state-of-the-art survey of malware detection approaches using data mining techniques. Hum-Centric Comput Inf Sci 2018;8:3. doi:10.1186/s13673-018-0125-x.
[40] Rudd EM, Rozsa A, Günther M, Boult TE. A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. IEEE Commun Surv Tutor 2017;19:1145–72. doi:10.1109/COMST.2016.2636078.
[41] Walker-Roberts S, Hammoudeh M, Dehghantanha A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access 2018;PP:1–1. doi:10.1109/ACCESS.2018.2817560.
[42] Liu V, Tesfamicael AD, Caelli W, Sahama T. Network security metrics and performance for healthcare systems management. 2015 17th Int. Conf. E-Health Netw. Appl. Serv. Heal., 2015, p. 189–94. doi:10.1109/HealthCom.2015.7454496.