Security Management in Health Care Information Systems

A literature review

Berglind Fjola Smaradottir
Department of Information and Communication Technology
Centre for eHealth
Faculty of Engineering and Science
University of Agder
N-4879 Grimstad, Norway
berglind.smaradottir@uia.no

***Abstract*—Health care information systems play an important role for communication across the organizational borders of health care services. The electronic health record represents the main entity in the management, exchange and storage of medical information. Health care organizations must adopt strategies for security and privacy risks associated with access to health care information systems, but on the other hand, the information needs to be accessible and readable for authorized health care professionals carrying out patient treatment. This paper presents a literature review on security management in health care information systems. The aim was to analyze descriptions and definitions of information security policy, access control management and the usability of security solutions.**

Keywords—access control; electronic health records; health care information systems; information security; usability

I. INTRODUCTION

Health care information systems play an important role in all communication and coordination processes of health care services and organizations. High-level goals for health care services are to maintain cross-disciplinary continuity of care for the patients by promoting cooperation and achieving greater cost-effectiveness by spending smarter [1]. The development of information technology, with the transition from paper-based health records to the electronic health records impacts on clinical workflow and daily routines in health care services. The implementation of electronic health records has improved interdisciplinary access to medical information at the point of care, which impacts on the quality and efficiency of treatment [2]. The electronic health record has been defined as the main fundamental entity for storing, sharing and analyzing medical information for management and decision making in health care organizations [3]. There is a trend on development and implementation of nationwide centralized databases of essential health care information about the patients and making the information accessible for health care professionals across the organizational borders in health care services [4][5][6]. Health care professionals are authorized to read and write information into the database. Within emergency care, improved access to updated health care information has potential as decision support, reduction of medication errors and avoiding unnecessary charge into hospital [7]. There is also an international trend on personal health records that are stored in the cloud, enabling people to access, manage and share their personal health information [8][9].

The implementation and the use of different kinds of electronic health records and information systems introduce challenges to privacy and security management in both personal care and health care organizations. Health care organizations and other providers of services have to adopt strategies to deal with security and privacy risks associated with access to health care information systems. On the other hand, the information needs to be accessible and readable for authorized health care professionals, in order to secure proper treatment for the patient. Most health care organizations and other service providers have implemented security solutions and authorization management. Access control implementations require education of the users and impacts on workflow and daily routines for health care professionals. The perceived usability of access control solutions impacts on the barrier of acceptance [10].

This paper presents an analysis of the security policy, access control management and the usability of security mechanisms in health care information systems based on literature review from a health informatics perspective.

The following three research questions (RQs) were addressed for this study:

RQ1: How is the security policy handled related to health care information systems?

RQ2: What kind of access control models are used for health care information systems?

RQ3: How is the usability described regarding security mechanisms for health care information systems?

Following this introduction, the research methodology is presented. The results of the literature review are presented, followed by a discussion. In last section, a summary on the study contribution and conclusions are drawn.

II. Methodology

The objective was to study security management in health care information systems. To answer the research questions, a literature search was made in Scopus and Google Scholar with search terms such as electronic health records, security management, access control and usability. 20 papers reflecting different aspects of security management in health care information systems were chosen. The abstracts were analyzed and finally 10 papers, with most relevant topics regarding information security, access control and usability in electronic health records, were included to be analyzed in the literature review, see Table 1.

TABLE I. Included Publications

Authors	*Title*	*Publisher*
Ferreira A, Correia R, Chadwick D, Antunes L.	Access control in healthcare: the methodology from legislation to practice.	Stud Health Technol Inform
Ferreira A, Correia R, Chadwick D, Antunes L.	Improving the implementation of access control in EMR	IEEE International Carnahan Conference on Security Technology
Hansen F, Oleshchuk V.	Application of role-based access-control in wireless healthcare information systems.	Scandinavian Health Informatics Conference
Smith E, Eloff JHP.	Security in health-care information systems-current trends.	Int J Med Inform
Blobel B.	Authorisation and access control for electronic health record systems.	Int J Med Inform
Blobel B, Nordberg R, Davis JM, Pharow P.	Modelling privilege management and access control	Int J Med Inform
Alhaqbani B, Fidge C.	Access control requirements for processing electronic health records	LNCS, Springer
Win KT.	A review of security of electronic health records.	HIM Journal
Li M, Yu S, Ren K, Lou W.	Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings	LNICST, Springer
Ferreira A, Antunes L, Chadwick D, Correia R.	Grounding information security in healthcare	Int J Med Inform

As a criterion for inclusion, the papers had to be written in English and be relevant for the research questions. The full version of the articles was accessed, printed out and thoroughly read. In the next step, the selected papers were read again and in order to extract data the content of each paper was classified into four thematic groups: 1) information security in health care information systems, 2) access control policies in health care information systems, 3) usability of security mechanisms in health care information systems, see Figure 1.

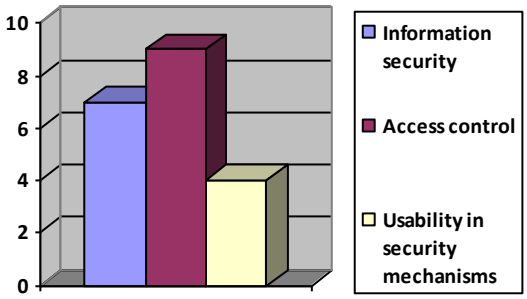

Fig. 1. Number of papers describing each sub-theme.

III. Results

The literature review showed that security policy in health care services is influenced by legal, organizational and technical issues [11][12], with the main aim to protect patient privacy and confidentiality. In multi-disciplinary organizations, the electronic health record is the core application in use [11].

A. Information Security in Health Care Information Systems

Health care services are becoming are becoming increasingly dependent on information technology, and the health care professionals need access to up-dated information in the treatment and care of patients [13]. Medical information is stored in databases, creating challenges with respect to security and privacy [11]. Most health care services have implemented security polices and existing security models were designed for requirements in controlled environments such as hospitals [14]. Security policy defines how to produce, store and use sensitive health care information in an organization. There are three ways of expressing a security policy; 1) verbally unstructured, 2) structured by schemas or 3) formal models [11]. A security policy is used to control access, authentication for requested data and protect security of sensitive data. Information security is defined with the characteristics confidentiality, integrity and availability [12]. Confidentiality in electronic health record is information privacy, which means that access is limited to authorized users. The most common authentication model in health care services is identifier and password. Audit logs are important as authorized users can misuse access rights and cause security breaks [12].

When protecting health care information, there are two types of cryptography that can be used; 1) secret key cryptography, where the same key is used for encryption and decryption and 2) asymmetric or Public Key Infrastructure (PKI) that uses two different keys, one for encryption and another for decryption [12]. But cryptography has some

constraints; not following what data is transferred and who accesses the data in both ends of the communication. Security models are so far designed regarding security requirements in controlled environment as a hospital, nationwide systems address other requirements [15].

For health care information systems, risk-analysis and risk-assessment must be done to identify threats to security management and determine consequences for the health care organization. Also, the likelihood of incidents needs to be evaluated with classification of grade of severity [13]. Integration of health care information systems between organizations requires access levels, with the implication to maintain health information confidentiality. Integrity means prevention of unauthorized changes of stored information, since inaccuracies can impact on the outcome of health care processes. Availability refers to that health care information has to be available for health care professionals at the time when requested [12].

For communication and interoperability between health networks and health care organizations, it is important to model authorization and access control based on architecture using international standards. This requires information exchange based on PKI and with a privilege and access control infrastructure. The standards ISO TC 215 and ISO TC 251 are dedicated to health informatics [11] Also, the standard CEN ENV 13608, Health Informatics- security for healthcare communication, describes a concept for security and terminology [14].

The development of nationwide electronic health record systems provided by a centralized database, where one single access point gives access to multiple patient data creates new risks for patient privacy and data security [15]. The trend on personal health records with storage in the cloud raises concerns on privacy and confidentiality. In traditional health care information systems, the health organization is responsible for information security. When introducing patients/citizens as administrators for storage of personal health information introduces new security and privacy risks. Existing cryptographic access control schemes; symmetric key and public key infrastructure, are designed for single-owner scenario and cause key management problem [16].

B. Access Control in Health Care Information Systems

Access control means limitation of legitimate operations for a user of a computer system. There are three traditional security models for access control; Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-based Access Control (RBAC). DAC restricts access to objects based on identity of group as they belong to. MAC means that access rights are given by a central authority, such as military security. RBAC means access is based on the role of user in the organization and different kinds of access are grouped by role name [11][13][15].

Access control in health care information systems has the implication to control who grants access to data based on the need-to-know-principle and protect information from unauthorized modification [15]. In general access-control consists of two parts; authentication and authorization. Access-control has the purpose to protect sensitive patient information. Two aspects are important; deny access to those users that have not right to read information and give access to relevant data regarding the need-to-know-principle [13]. Role-based access control was described as the most used model for authorization management in health care information systems. Roles are based on competencies, credentials and responsibilities in the organization. Role-based access control simplifies the administration and management of privileges and roles in complex organizations [17]. All users are assigned roles and the use of resources is restricted to the authorization of the user. Role-based access control is used in advanced health care information systems because it provides the ability of a fine-grained access policy that is possible to administrate for a large number of human resources [15].

Access to patient information is restricted to health care professional involved in treatment. The professionals with closest distance to patient will have least privilege restrictions. Different health care professions have different access rights, for instance physicians, nurses and secretaries [11][14]. Audit logs are implemented since incidents of data breaks show misuse by authorized users [13][15][17][18][19].

In emergency situations, the access rights for the user-role of specially authorized health care professionals can be redefined. “Emergency access” or “break-the-glass access” means immediate access to patient’s medical information. This is to be used in emergency care and scenarios where time is limited for decisions on emergency treatment [13][14][15][16].

C. Usability of Security Mechanisms

Access control solutions in health care services often create a barrier of acceptance and they are linked to usability problems, impacting on clinical practice and workflow. Access control policy should be designed and deployed regarding the needs and workflow of the health care professionals to cause fewer problems for health care professionals to access relevant information related to the work duties and would enhance efficiency. In the design of access control solutions, end-users should be invited to participate in the process in order reduce barrier of acceptance, make implementation and education on the use of the access control solution easier. Use of focus groups and questionnaires were proposed to gather information on needs and workflow for the design process, to make implementation of security solutions more likely to succeed and decrease educational and workflow problems [18][19][20].

IV. DISCUSSION

This paper has presented a literature review on security management in health care information systems with a focus on information security, access control and usability issues related to security solutions.

The three research questions (RQs) formulated at the beginning of this paper are answered below based on the results from the study.

About the RQ1 asking about how security policy is handled in health care information systems. The findings of the review showed that health care information systems and

communication technology play a fundamental role in the management of health care services. Access to clinical information at the point of care, as well as exchange of information between health care organizations, are important aspects when defining security policy. The nature of health care information, stored in databases or in the cloud, raises several concerns on information security. The review found that security policy is influenced by legal, organizational and technical issues, with the main aim to protect patient privacy and confidentiality of personal health information. Existing security models are designed for requirements in controlled environment such as hospitals. Nationwide systems or storing in the cloud addresses other requirements and create challenges for patient privacy and data security. Integration of health care information systems between organizations requires implemented communication security solutions.

RQ2 asked about access control models. The review concluded that role-based access control makes the management of privileges and roles easier in complex settings like hospitals, with multiple user groups in different positions and responsibilities. Audit logs are implemented since incidents of data breaks show misuse by authorized users. This illuminates that the users are a weak link in the system. Access to electronic health records is supposed to reduce errors in medical treatment, but health care professionals can make unauthorized actions which can impact on accuracy and security in the medical treatment.

Regarding RQ3, on usability of security mechanisms, the review revealed that security solutions in health care services are linked to usability problems. Workflow problems are related to human interactions with the security solution. Other studies [10][21] have shown that health care professionals redesign their workflow processes when using electronic health records, and that has impacts on information security. Health care professionals have described log in procedures to electronic health record as time-consuming. This causes workarounds such as not reading patient information before consultations or care, and information is read or written into patient's record in the name of a colleague which is logged in.

The execution of this literature review has some limitations such as a reduced number of included papers, but on the other hand, all the included papers presented relevant aspects of security management in health care information systems.

V. Conlusion

The reviewed literature concluded that security policy in health care information systems is used to control access and authentication and defines how to create, store and use sensitive health care information in order to protect patient privacy and confidentiality. The impacts of security policy on clinical workflow should be studied further. As a future work, a user-centered design approach [22] with active end-user involvement in the definition and development of access control solutions should be carried out. User evaluations should be made both in laboratory and real hospital environments to study the usability of access control solutions and how they impact on clinical work processes.

Acknowledgment

The author thanks Vladimir Oleshchuk, Professor in Information Security, for collaboration and discussions during the early phases of the literature review process.

References

[1] European Commission, Communication from the Commission- On effective, accessible and resilient health systems, 2014. [retrieved: October, 2017]. Available from:https://ec.europa.eu/health//sites/health/files/systems_performance_assessment/docs/com2014_215_final_en.pdf

[2] N. Menachemi, H.C. Taleah, "Benefits and drawbacks of electronic health record systems," Risk Manag Healthc Policy, 4(47), 2011, doi: 10.2147/RMHP.S12985

[3] U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. [retrieved: October, 2017]. Available from: https://www.healthit.gov/patients-families/basics-health-it

[4] W. Dorda, G. Duftschmid, L. Gerhold, W. Gall, J. Gambal, "Austria's path toward nationwide electronic health records," Methods Inf Med, 47(2), pp. 117-123, 2008.

[5] Takemura, Tadamasa, et al. "Development of fundamental infrastructure for nationwide EHR in Japan, "J Med Syst, 36 (4), pp. 2213-2218, 2012.

[6] K. Bernstein, M. Bruun-Rasmussen, S. Vingtoft, S.K. Andersen, C. Nøhr, "Modelling and implementing electronic health records in Denmark," Int J Med Inform, 74(2), pp. 213-2, 2005.

[7] Norwegian Summary Care Record. [retrieved: October, 2017]. Available from: https://helsenorge.no/kjernejournal/kjernejournal-for-safer-healthcare

[8] G. Hsieh, R.J. Chen, "Design for a secure interoperable cloud-based Personal Health Record service," In IEEE 4th International Conference on Cloud Computing Technology and Science, pp. 472-479, 2012.

[9] A. Kaletsch, A. Sunyaev, "Privacy engineering: personal health records in cloud computing environments," Computing Environments ICIS, 2011.

[10] A. Faxvaag, T.S. Johansen, V. Heimly, L. Melby, L.A. Grimsmo, "Healthcare professionals' experiences with EHR-system access control mechanisms," Stud Health Technol Inform, 169, pp. 601-605, 2011.

[11] B. Blobel, "Authorisation and access control for electronic health record systems," Int J Med Inform, 73(3), pp. 251-257, 2004.

[12] K.T. Win, "A review of security of electronic health records," Health Inf Manag J, 34(1), pp. 13-18, 2005.

[13] E. Smith, J.H. Eloff, "Security in health-care information systems—current trends;" Int J Med Inform, 54(1), pp. 39-54, 1999, doi: https://doi.org/10.1016/S1386-5056(98)00168-3

[14] B. Blobel, R. Nordberg, J.M. Davis, P. Pharow, "Modelling privilege management and access control," Int J Med Inform, 75(8), pp. 597-623, 2006, doi: https://doi.org/10.1016/j.ijmedinf.2005.08.010

[15] B. Alhaqbani, C. Fidge, "Access control requirements for processing electronic health records," LNCS, vol. 4928, Springer, pp. 371-382, 2007.

[16] M. Li, S. Yu, K. Ren, W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," LNICST, vol 50, Springer, pp. 89-106, 2010.

[17] F. Hansen, V. Oleshchuk, "Application of role-based access control in wireless healthcare information systems," In Scandinavian Conference on Health Informatics, pp. 30-33, 2003.

[18] A. Ferreira, R.J.Correira, D.W. Chadwick, L. Antunes, "Access control in healthcare: the methodology from legislation to practice," Stud Health Technol Inform, 160, pp. 666-670, 2010.

[19] A. Ferreira, R. Cruz-Correia, D. Chadwick, L. Antunes, "Improving the implementation of access control in EMR," In 42nd annual IEEE

International Carnahan Conference on Security Technology, pp. 47-50, 2008.

[20] A. Ferreira, L. Antunes, D. Chadwick, R. Correia, "Grounding information security in healthcare," Int J Med Inform, 79(4), pp. 268-283, 2010, doi: https://doi.org/10.1016/j.ijmedinf.2010.01.009

[21] B. Smaradottir, "Communication and information exchange in hospital wards: The role of electronic nursing documentation," Proceedings of ITCH2017, Victoria, BC, February 2017.

[22] B.F. Smaradottir, "The steps of user-centered design in health information technology development- recommendations from a PhD research study," 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2016, pp. 116-121, doi:10.1109/CSCI.2016.0029