

A literature review: Security Aspects in the Implementation of Electronic Medical Records in Hospitals

Piping Asgiani^{1*}, Chriswardani Suryawati², Farid Agushybana³

¹Diponegoro University, Jl. Prof Soedarto, SH, Tembalang, Semarang, Central Java, email: pipingasgiani@gmail.com, Indonesia

²Diponegoro University, Jl. Prof Soedarto, SH, Tembalang, Semarang, Central Java, email: chriswardani@lecturer.undip.ac.id, Indonesia

³Diponegoro University, Jl. Prof Soedarto, SH, Tembalang, Semarang, Central Java, email: agushybana@lecturer.undip.ac.id, Indonesia

ABSTRACT

Backgrounds: Electronic Medical Records have complete and integrated patient health data, and are up to date because RME combines clinical and genomic data, this poses a great risk to data disclosure. The priority of privacy is data security (security) so that data will not leak to other parties. That way cyber attacks can be suppressed by increasing cybersecurity, namely conducting regular evaluation and testing of security levels.

Objectives: To determine the security technique that maintains privacy of electronic medical records.

Methods: This type of research uses a literature review method

Results: Data security techniques are determined from each type of health service. Data security techniques that can be applied are cryptographic methods, firewalls, access control, and other security techniques. This method has proven to be a very promising and successful technique for safeguarding the privacy and security of RME

Conclusion: Patient medical records or medical records are very private and sensitive because they store all data about complaints, diagnoses, disease histories, actions, and treatments about patients, so the information contained therein must be kept confidential. As well as the hospital as a medical record manager is required to apply for patient privacy data security techniques.

Keywords: *Electronic Medical Record, Privacy, Security*

INTRODUCTION

In this era of globalization, technological developments in the health care sector are very rapid. In Indonesia, the use of information technology in the field of health services is used for Health Information Systems (SIK) and currently health care facilities use information technology for the management of patient medical records.

The sophistication of information technology in managing patient medical records refers to the application of the Electronic Medical Record (RME). The implementation of this Electronic Medical

Record is intended as a means that supports convenience for health services and is expected to have a positive impact on the services provided to patients.¹

Electronic Medical Record (RME) is an electronic record or record regarding a person's health information that is created, stored, and managed by medical personnel and health workers who have rights in health service organizations.² RME has many advantages such as easy storage and can be used for clinical decision making.³

Electronic Medical Records have complete and integrated patient health data,

and the latest because RME combines clinical and genomic data, this poses a great risk to data disclosure. Especially if RME is used by many users and is integrated with external parties.⁴

Information about patient privacy along with their medical data will only be legalized if it is in accordance with what is stated in the law, in addition to these provisions, it can be said to be an act of leaking secrets that is against the law, because it results in material and immaterial losses for the patient. Violation of the law related to this may be subject to civil sanctions, that's chapter 1365, 1366, and 1367 KUHP; Criminal Law, that's chapter 112 and 322 KUHP; and administrative sanctions in accordance with Government Regulation of the Republic of Indonesia Number 10 of 1966, even though the patient has apologized and did not take the case to the authorities.

Published by the DHS Cybersecurity and Infrastructure Security Agency (CISA) a report on 21 vulnerabilities in popular medical devices. Most of the problems related to the confidentiality of electronic protected health information (ePHI) or electronic medical records. There is one big problem, namely the potential for patient identity breaches. Losses in costs that must be borne by health care providers to address this problem ranged from US \$ 6.45 million per incident. The problem does not stop at ePHI and recovery costs, it is possible for

attackers to change the patient's treatment status information.

In this case, it is necessary to strengthen the understanding of cybersecurity, given the enormous loss caused by the crime of the world of information technology on patient data, electronic medical records, which are very private and sensitive. The priority of privacy is data security (security) so that there will be no data leakage to other parties. In this way, cyber attacks can be suppressed by increasing cybersecurity by evaluating and testing the security level on a regular basis.⁵

The existing regulations in Indonesia regarding the protection of personal data and maintaining the confidentiality of patient data are regulated in the Regulation of the Minister of Health Number 269 of 2008, the Information and Electronic Transactions Law (ITE), and the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic System. The limitation of this regulation is that it only regulates the legal aspects of the implementation of RME, but has not thoroughly explored the privacy issues of RME data. As a reference in overcoming the problem of RME privacy, will be discussed in the literature review on RME data security techniques in protecting RME privacy.

RESEARCH MATERIALS AND METHODS

The type of research used is a

literature study on security systems for privacy protection in RME. The literature study used in this study is limited to the data security techniques applied with regard to privacy protection in RME. The journals used in the literature review were obtained through the database of the International PubMed journal providers, and Science Direct, while the National journals were through Google Scholar.

The author uses the keywords Privacy in Electronic Medical Records, Security in Electronic Medical Records, Implementation of Electronic Medical Records, for international journals, while national journals use the keywords Privacy in Electronic Medical Records, Security of Electronic Medical Records, and Application of Electronic Medical Records. Found 15 international journals and 8 national journals, then the authors limit based on articles relevant to keywords, obtained 7 from International journals and 3 from National Journals.

RESULTS AND DISCUSSION

One of the uses of information technology is data sharing, which is to make it easier for patients to undergo health checks in several health services. Although data sharing can provide convenience to patients, data sharing should be carried out with the patient's knowledge so as not to cause problems in the future. In data sharing, it is also necessary to pay attention

to data privacy.

Several parties who are closely related to patient data privacy are doctors and other health workers who have access to patient data and information, including managerial health facilities, health care financing officers, other health workers who have access to patient data and information, legal entities, students and students in charge of examination, treatment, care, and or information management in health facilities.⁵

In an effort to maintain the security of patient data privacy in electronic medical records, it is necessary to provide standard operating procedures (SPO) regarding the protection of privacy and patient medical data, adapted to the type and strata of each health service facility and the application of a patient privacy data security technique. Based on 10 journal articles that have been obtained, here are the results of the literature review:

Table 1. Data security and privacy on RME

No	Writer	Study
1	Al-Shaher, (2017) ⁶	Implement patient privacy data security techniques by implementing firewalls, passwords, and access controls
2	Amer, (2015) ⁷	The security techniques applied use data encryption, passwords, and perform periodic system backups.
3	Chaturvedi et al, (2017) ⁸	Implement the RME data privacy mechanism in the form of an authentication scheme with Self-Identity. If the viewer is not authorized, it will not be able to access any data in RME. Or restricted access according to their respective IDs.
4	Huang et al, (2010) ⁹	Implement a security system with features that can hide data from parties who do not have the authority, or can only display data according to the authority of the accessor.
5	Jannetti, (2014) ¹⁰	Implement various patient privacy data security techniques by RME data encryption and decryption,

No	Writer	Study
		Firewall, Audit Log, as well as for direct supervision by a Chief Information Security Officer
6	Carvalho & Paiva (2017) ¹¹	Using role-based access control (RBAC).
7	Senese, (2015) ¹²	Implement role-based and authenticate each user with encryption
8	Nuryati, (2015) ¹³	Not implementing a security system to maintain the security of privacy data, in the sense that patient data stored electronically can be accessed by anyone.
9	Rusli, (2010) ¹⁴	Using electronic signature
10	Setiawan et al, (2020) ¹⁵	A blockchain mechanism with access rights for each user, and a multi-user rest server where the accessor is required to have a network card.

Encryption technique is one part of cryptography, namely: Confidential or sensitive information can be changed from an understandable form to an incomprehensible form. Data security techniques with encryption increase security when the data exchange process occurs in the information system, by decrypting the RME data that will be accessed using a key. One of the decryption techniques is the use of digital signatures.¹⁰

Privacy data security techniques with digital signatures are needed with the aim of providing authentication and safeguarding the privacy of the content in it. Digital signatures are the key to this aspect, with technological advances, the level of confidentiality and security of digital signatures continues to be higher and more secure. Without a digital signature, electronic medical records will become a hole in the privacy of patient data, which should be fully protected by the hospital. This can threaten the social, psychological, and even life status of the patients being treated.¹⁵

The affixing of electronic signatures can use an information system, or by using a worksheet application or the latest plugin that also supports electronic signing, which has been widely circulated in the world today. The ease of getting this application does not affect the level of data privacy protection, because the digital signature for each document is very different for other documents.

The most commonly used data security technique is using a firewall.^{6,10} A firewall is a paid security system with prices varying depending on the size and scope of the organization using it. But the performance of this security system is quite satisfactory because it has proven successful in securing the network and can protect RME data security.¹⁶

In addition, data security techniques that can be applied are by adding a hide feature to regulate what data should be displayed and what data should be hidden according to the authority of the party with access.⁹ The division of authority can be done by granting access control to restrict access to RME data. This access control can be in the form of a password and PIN number, for example, user X can only view it, then user Y is given access rights to view and edit RME data.

Another access control is using role-based access control (RBAC). This method gives permission to the user to access the data according to their role in

the health care organization. From various health workers, they are distinguished according to their roles, for example: doctors, nurses, patients, and administrative officers.¹²

However, from research,¹³ it was found that the electronic medical record system that was running had not implemented a system to maintain patient privacy because it could be accessed by each medical staff and could easily view the desired patient data even though it was not a patient being treated.

Judging from the development of RME in Indonesia, there are still few hospitals that implement a patient privacy data security system. If viewed, the application of RME is only limited to the storage and exchange of patient data that can be done quickly.

From the literature study that has been carried out, the authors expect support from the government in the form of a clear legal umbrella regarding the use of data security systems to protect the privacy of such sensitive patients. In addition, moral support from the government such as socialization to hospitals throughout Indonesia about the security of patient privacy data, because the government is a role model for the community and organizations.

CONCLUSION

The patient's medical record or

medical record is very private and sensitive because it stores all data about complaints, diagnoses, disease history, actions, and treatments about patients, so the information contained therein must be kept confidential. And hospitals as medical record managers are required to apply patient privacy data security techniques to avoid leakage of medical data that leads to material and non-material losses.

Data security techniques that can be applied are the following methods: cryptography, firewalls, access control, and other security techniques. This method has proven to be a very promising and successful technique for maintaining privacy and security of RME. It is recommended that health service institutions that implement RME not only focus on the benefits of implementing RME, but the important thing is to maintain the security and privacy of RME data with proven security techniques.

ACKNOWLEDGMENTS

1. Kuswanto Hadjo, dr., M.Kes, Dean of the Faculty of Health, Universitas Jenderal Achmad Yani Yogyakarta, email: info@fkes.unjaya.ac.id.
2. Dian Puspitasari, M.Keb, Head of PPPM, Faculty of Health, Universitas Jenderal Achmad Yani Yogyakarta, email: info@fkes.unjaya.ac.id.

LITERATURE

1. Sittig, D., Gonzales, D., and Singh, H. Contingency planning for electronic

- health record-based care continuity: a survey of recommended practices. *International Journal of Medical Informatics*. 07 August 2014. Volumes. 83, p. 797–804.
2. Saif, S., Wani, S., and Khan SA Network engineering solution for data sharing across healthcare providers and protecting patients' health data privacy using EHR system. *Journal of Global Research in Computer Science*. 08 August 2011. Volumes. 2.
 3. Shabo, A. The implications of electronic health records for personalized medicine. *Personalized Medicine*. 12 August 2005. Volumes. 2, p. 251-258.
 4. Brothers, KB and Rothstein, MA Ethical, legal and social implications of incorporating personalized medicine into healthcare, *Personalized Medicine*. 01 November 2015. Volumes. 12, p. 43–51.
 5. Budiyantri, RT, Arso, SP, and Herlambang, PM Cloud-Based Electronic Medical Record. *Mirror of the World of Medicine Edition 268*. 2018. Volume. 45.
 6. Al-shaher, MA Protect Healthcare System Based on Intelligent Techniques. *Proceedings of 2017 4th International Conference on CoDIT*. 5-7 April 2017. p. 0421–0426.
 7. Amer, K. Informatics: Ethical Use of Genomic Information and Electronic Medical Records. *OJIN*. 08 May 2015. Volumes. 20
 8. Chaturvedi, A., Mishra, D., and Mukhopadhyay, S. An enhanced dynamic ID-based authentication scheme for telecare medical information systems, *J. King Saud Univ. Comput. inf. Sci.*, January 2017. Volume. 29, p. 54–62.
 9. Huang, LC, Chu, HC, Lien, CY, Hsiao, CH, and Kao, T. Embedding a hiding function in a portable electronic health record for privacy preservation. *J. Med. syst.* June 2010. Volumes. 34, p. 313–320.
 10. Jannetti, MC In Focus: Safeguarding patient information in electronic health records, *AORN J*. 2014. Volume. 100, p. C7–C8.
 11. Carvalho, M. and Paiva PB Health Information System (HIS) Role-Based Access Control Current Security Trends and Challenges. *J. Healthc. eng.* February 2018. Volumes. 2018, pp. 1–8.
 12. Senese, SV A Study of Access Control for Electronic Health Records. *Open Portal to University Scholarships*. 2015.
 13. Nuryati and Widayanti, NA Evaluation of the Implementation of the Electronic Health Record (HER) System at the Gadjah Mada University Academic Hospital based on the PIECES Analysis Method. 2014.
 14. Rusli R. Digital Signature for Electronic Medical Records in the Medical World in Indonesia. 2010.
 15. Setiawan, EP, Bhawiyuga, A. and Siregar, RA Development of a Hospital Medical Record System with a Permissioned Blockchain-based Multi User Rest Server using the Hyperledger Framework. *JPTIHK*. 7 February 2020. Volumes. 4, p. 01–10.
 16. Kruse, CS, Smith, B., Vanderlinden, H., and Nealand, A. Security Techniques for the Electronic Health Records. *J. Med. syst.* August 2017. Volumes. 41.