PRIVACY ISSUES IN ELECTRONIC MEDICAL RECORD IN INDONESIA : A Review

Syamsuriansyah[1, a)] and Hizriansyah[2, b)]

[1,2] *Medical Record and Health Information, Politeknik Medica Farma Husada Mataram, Indonesia*.

[a)]Corresponding author: sam_bptk@yahoo.com
[b)]hizriansyah@politeknikmfh.ac.id

Abstract. The Electronic Medical Record (EMR) is a breakthrough in the use of information technology in healthcare that aims to improve health services. The number of healthcare providers using EMR, which must take into account not only the problem of data migration from analog to digital, but also how to secure data on EMRs that privacy issues have not been adequately addressed and handled making the process of this EMR. To address the issue, the researcher conducted a review of the literature on data security techniques in 20 articles, proceedings, and journals. Cryptography, firewalls, and access control are common data security techniques used in an effort to secure data.

INTRODUCTION

Electronic medical records have been promoted as a panacea for many of the problems that plague primary care [1]. Others have criticized the shift to electronic medical records (EMR) as a threat to the physician-patient relationship, a violation of patient privacy, and an additional administrative burden on the health-care system, all of which contribute to physician burnout [2] [3]. A modern EMR is more than just a digitized paper chart. Rather, it is a digital application that can actively interact with providers and patients and is made up of a series of data fields that can be analyzed, processed, and reported on to support communication, appropriate clinical interventions, quality improvement, and patient safety [4].

The privacy rule governs the use of health data and establishes standards for entities working with health data to follow in order to protect patients' private medical information [5]. Paper-based documentation in the healthcare sector has been replaced by digital documentation, in which patient information is transferred electronically from one location to another. However, there are still challenges and problems in this domain that must be addressed due to a lack of proper standards that have not regulated the privacy of electronic medical record [6].

This has been proven by the sale of patient data at the University of Chicago Hospital and Wilcox Memorial Hospital, Kauai, Hawaii (as much as 130,000 patient data). As previously mentioned, EMR is one of the breakthroughs in the use of information technology in the health sector which is currently being intensively developed in Indonesia, this is associated with the understanding of users involved in health services regarding cyber-security. Understanding of cyber-security is very much needed in the use of information technology in the health sector, especially in the development of this RME. This is due to the sensitive nature of the information stored in EMR, and so far privacy issues have not been adequately regulated and handled in the process of making this EMR

METHOD

This type of research is a literature study on privacy issues in RME. The literature study conducted in this study was limited to the techniques applied to maintain data security which correlated with privacy issues in RME. The literature used in this paper is proceedings and journals from PubMed, IEEE, and Science Direct. Proceedings and journals used use the keywords "Security in Electronic Medical Record", "Access Control in Electronic Medical

Record", "Privacy Issues in Electronic Health Record", "Firewall in EMR". From the search results found 20 articles that match the keywords.

Standards regarding exchange, integration, sharing and retrieval of electronic health information that support clinical practice and the management and evaluation of health services are regulated by a non-profit body, namely Health Level Seven International (HL7). HL7 focuses on how data is transmitted from one service to another. In addition to the HL7 rules, the confidentiality and security of protected health information, including RME in America, is discussed in the Health Insurance Portability and Accountability Act (HIPAA) [5]. However, in fact the security requirements end-to-end is more complex than stated in HL7 [7] [8]. This is complicated by the sensitivity of medical record data which is confidential data and cannot be disseminated freely [9], [10].

By utilizing information technology, one of which is the use of internet media as one of the uses of technology in facilitating access to data making it easier for patient medical record data to be hacked by irresponsible parties. In May 2017, the WannaCry malware infected hundreds of hospital information systems throughout Europe, to store medical record data for all patients, then demanded a ransom if the data was to be returned [11]. It was stated in research [12] that 70% of people are worried if health information about them is leaked. This has been proven by the sale of patient data at the Hospital. University of Chicago Hospital and Wilcox Memorial Hospital, Kauai, Hawaii (130,000 patient records). From this incident it shows that even though RME is a good solution for presenting and processing data in real-time, it still has a problem that is how data is stored and flows through the system safely and kept confidential.

DISCUSSION

Based on 20 journal articles and proceedings obtained by searching based on the keyword "security and privacy issues in electronic medical records" it can be seen that data security techniques and information systems in RME data and health network is by utilizing techniques from cryptography

Table 1.

Penulis	Teknik Keamanan
[8]	Menerapkan *Document Archiving and Communication System* untuk menjaga keamanan dan interoperabilitas dari RME dan dokumen klinis lainnya.
[7]	Memanfaatkan tiga level keamanan dalam XML, yaitu 1. XML *Key Management Services* (tanda tangan digital untuk mengautentifikasi pesan dari sumber data) 2. XML *Encryption* (untuk melindungi keamanan data yang dikirim) 3. XML *Key Management Services* (pendaftaran kunci publik dan validasi)
[13]	Penerapan *firewall* untuk pengamanan data
[14]	Enkripsi pada data RME, *password* dan *backup* sistem
[15]	Memberikan fitur *hide* (sembunyi) untuk mengatur mengenai data RME apa saja yang dapat ditampilkan atau disembunyikan dari pihak-pihak yang memiliki wewenang yang berbeda.
[16]	Enkripsi data, dan membuat data RME menjadi anonimus, jika data tersebut diambil untuk penelitian
[17]	*Firewall*, enkripsi dan dekripsi data RME, Audit Log, serta untuk menjaga keamanan data, data-data RME diawasi oleh seorang *Chief Information Security Officer*
[18]	Penerapan *role-based* dan autentifikasi personal dengan menggunakan enkripsi
[13]	*Password*, kontrol akses dan *firewall*

[8]	Kontrol akses, Penyimpanan data dengan menggunakan Enkripsi, Audit untuk mengetahui siapa saja yang mengakses data dan apa saja perubahan yang dilakukan
[19]	Kontrol akses, Fungsi Log Audit untuk mengetahui kegiatan apa saja yang dilakukanpada data RME, Fungsi Agregasi data
[20]	Keamanan dengan menggunakan *role-based*
[21]	*Role-Based Access Control* (RBAC)
[22]	Skema autentifikasi dengan penggunaan ID
[23]	Kriptografi (tanda tangan digital, algoritma enkripsi, sertifikasi digital)
[24]	*Mobile agents*
[25]	Protokol kriptografi matriks RBAC
[26]	Tanda tangan digital
[27]	*Cloud computing*
[28]	Kontrol akses untuk mencegah orang yangtidak bertanggung jawab mengakses data RME.

Encryption and decryption are part of cryptography, namely confidential or sensitive information can be changed from an understandable form to an incomprehensible form [29]. The form of information that can be understood is called plaintext, meanwhile The form of information that cannot be understood is called ciphertext. The process of changing the form of information from plaintext to ciphertext is called encryption, and vice versa is called decryption using a key [8].

Data security techniques with encryption increase security when data exchange processes occur in information systems. With this encryption, the accessed RME data must be opened by decrypting it using a key. One of the decryption techniques is to use a digital signature. This method has been proven to protect data from security breaches [14]. Furthermore, encryption and decryption are also successful methods of securing data on Personal Health Information (PHI) by accessing a mobile agent. Mobile agent is software that can transfer data from one computer to another automatically, and this function can be executed even if the user is not connected to the network [28]. By securing the mobile agent when data exchange occurs, RME is not only more secure but also easily accessible [24]. Another cryptographic technique is to use a username and password. Using a username and password can avoid security breaches, but users are advised to change passwords regularly. The password used must not have any meaning for the user, for example, date of birth. This is done to prevent hackers from easily guessing passwords.

In addition to the techniques previously mentioned, the most common security technique another use is the use of firewalls [13], [16], [9], [7]. Although firewalls in their implementation are expensive and vary based on the size and scope of the organization, this firewall has proven successful in securing the network and can protect RME data security [9].

Firewalls in network providers, whether in the form of hardware or software, act as a security buffer between the provider's network and "untrusted" networks, such as the internet. When placed on a network, a firewall can help ensure that only the right information and personnel are allowed access to the provider's network, block unwanted or malicious transmissions from unauthorized users, and can filter content that users are allowed to view. . With this behavior, the firewall is very functioning to secure confidential RME data.

Furthermore, a security technique that can be implemented is to provide a hide feature to control what RME data can be displayed or hidden from parties with different authorities. Then, the data security technique used is to apply access control to RME data.

This access control can be in the form of passwords and PIN numbers that can limit access to information. Access control contains the extent to which users are permitted to access RME data. For example, user A is given access to read, write and execute data, then user B is only given access to read data [30].

Another access control that is used is by implementing role-based access control (RBAC). This RBAC method allows users to access data according to their roles in health care organizations. The role assignment procedure is usually based on a needs evaluation and security policy. For example, for RME the user roles involved are nurses, doctors, patients and administrative staff [18]. Each of these roles has different access that is tailored to their role.

From the literature studies that have been carried out, it is hoped that in the process of developing RME which is being intensively carried out in the health sector, both government and private, it is not only concerned with migrating data from paper to digital to facilitate the work of medical recorders and to consider how data can be

presented appropriately so that information can be encoded. Only in real time, but behind that the security of data from patients must also be considered.

As we know, data in medical records is confidential, sensitive and private data for every patient that needs to be kept safe. This needs to be taken into consideration because it does not rule out the possibility that health information systems, especially RME that have been implemented by current health service providers, will be integrated with all health service providers everywhere, not limited by region. In this case the patient can visit any service provider with the same medical record number. In addition, existing health information systems can be integrated with other service providers, such as banks or insurance company. So that it is necessary to understand and apply data security techniques from an information technology perspective, which must be considered and implemented in the current system and a clear legal basis that regulates privacy regulations in RME needs to be established.

CONCLUSION

Electronic medical records contain information about patients and the results of diagnoses from health actions taken, most of which are considered as health information that must be protected. As explained, privacy and security are important in the implementation of RME, so data security techniques are needed that can protect the data and information contained therein.

Data security techniques that can be done are by utilizing cryptographic methods, firewalls, access control, and other security techniques. This method has proven to be a very promising and successful technique for maintaining the privacy and security of RME

REFERENCES

[1] National Coordinator for Health Information Technology (ONC), "Health IT and Health Information Exchange Basics," *HealthIT.gov*, 2022. https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/benefits-ehrs (accessed Nov. 25, 2022).

[2] F. Schulte and E. Fry, "Death By 1,000 Clicks: Where Electronic Health Records Went Wrong," *FORTUNE*, 2019. https://khn.org/news/death-by-a-thousand-clicks/ (accessed Nov. 25, 2022).

[3] D. Gorn, "These doctors think electronic health records are hurting their relationships with patients," *pbs.org*, 2021. https://www.pbs.org/newshour/health/doctors-think-electronic-health-records-hurting-relationships-patients (accessed Nov. 25, 2022).

[4] R. S. Janett and P. P. Yeracaris, "Electronic medical records in the american health system: Challenges and lessons learned," *Cienc. e Saude Coletiva*, vol. 25, no. 4, pp. 1293–1304, 2020, doi: 10.1590/1413-81232020254.28922019.

[5] W. Moore and S. Frye, "Review of HIPAA, Part 1: History, protected health information, and privacy and security rules," *J. Nucl. Med. Technol.*, vol. 47, no. 4, pp. 269–272, 2019, doi: 10.2967/JNMT.119.227819.

[6] M. Ayaz, M. F. Pasha, M. Y. Alzahrani, R. Budiarto, and D. Stiawan, "The Fast Health Interoperability Resources (FIHR) Standard: Systematic literature review of implementations, pplications, challenges and opportunities," *JMIR Med. Informatics*, vol. 9, no. 7, pp. 1–21, 2021, doi: 10.2196/21929.

[7] P. Ray and J. Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," *Annu. Int. Conf. IEEE Eng. Med. Biol. - Proc.*, pp. 4686–4689, 2006, doi: 10.1109/IEMBS.2006.260862.

[8] J. Delgado, S. Llorente, M. Pàmies, and J. Vilalta, "Security and privacy in a DACS," *Stud. Health Technol. Inform.*, vol. 228, pp. 122–126, 2017, doi: 10.3233/978-1-61499-678-1-122.

[9] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security Techniques for the Electronic Health Records," *J. Med. Syst.*, vol. 41, no. 8, 2017, doi: 10.1007/s10916-017-0778-4.

[10] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," *Annu. Int. Conf. IEEE Eng. Med. Biol. - Proc.*, pp. 5453–5458, 2006, doi:

10.1109/IEMBS.2006.260060.

[11] M. M. Mello, J. Adler-Milstein, K. L. Ding, and L. Savage, "Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles?," *Milbank Q.*, vol. 96, no. 1, pp. 110–143, 2018, doi: 10.1111/1468-0009.12313.

[12] D. F. Sittig, D. Gonzalez, and H. Singh, "Contingency planning for electronic health record-based care continuity: A survey of recommended practices," *Int. J. Med. Inform.*, vol. 83, no. 11, pp. 797–804, 2014, doi: 10.1016/j.ijmedinf.2014.07.007.

[13] M. A. Al-Shaher, R. T. Hameed, and N. Ţăpuş, "Protect healthcare system based on intelligent techniques," *2017 4th Int. Conf. Control. Decis. Inf. Technol. CoDIT 2017*, vol. 2017-Janua, pp. 421–426, 2017, doi: 10.1109/CoDIT.2017.8102628.

[14] L. B. Harman, C. A. Flite, and K. Bond, "STATE OF THE ART AND SCIENCE Electronic Health Records: Privacy, Confidentiality, and Security," *Am. Med. Assoc. J. Ethics*, vol. 14, no. 9, pp. 712–719, 2012, [Online]. Available: www.virtualmentor.org712.

[15] L. C. Huang, H. C. Chu, C. Y. Lien, C. H. Hsiao, and T. Kao, "Embedding a hiding function in a portable electronic health record for privacy preservation," *J. Med. Syst.*, vol. 34, no. 3, pp. 313–320, 2010, doi: 10.1007/s10916-008-9243-8.

[16] M. Shuchman, "Researcher-participant confidentiality now a formal concept in Canadian law.," *CMAJ*, vol. 186, no. 4, pp. 250–251, 2014, doi: 10.1503/cmaj.109-4717.

[17] A. Shenoy and J. M. Appel, "Safeguarding confidentiality in electronic health records," *Cambridge Q. Healthc. Ethics*, vol. 26, no. 2, pp. 337–341, 2017, doi: 10.1017/S0963180116000931.

[18] S. V. Senese, "A Study of Access Control for Electronic Health Records," 2015.

[19] A. Omotosho and J. Emuoyibofarhe, "A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records," *Int. J. Appl. Inf. Syst.*, vol. 7, no. 8, pp. 11–18, 2014, doi: 10.5120/ijais14-451225.

[20] M. A. De Carvalho Junior and P. Bandiera-Paiva, "Health Information System Role-Based Access Control Current Security Trends and Challenges," *J. Healthc. Eng.*, vol. 2018, 2018, doi: 10.1155/2018/6510249.

[21] M. . Rana, M. Kubbo, and M. Jayabalan, "Privacy and Security Challenges Towards Cloud Based Acces Control in Electronic Health Records," *Asian J. Inf. Technol.*, vol. 16, pp. 2–5, 2017.

[22] A. Chaturvedi, D. Mishra, and S. Mukhopadhyay, "An enhanced dynamic ID-based authentication scheme for telecare medical information systems," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 29, no. 1, pp. 54–62, 2017, doi: 10.1016/j.jksuci.2014.12.007.

[23] A. Tejero and I. De La Torre, "Advances and current state of the security and privacy in electronic health records: Survey from a social perspective," *J. Med. Syst.*, vol. 36, no. 5, pp. 3019–3027, 2012, doi: 10.1007/s10916-011-9779-x.

[24] M. Nikooghadam and A. Zakerolhosseini, "Secure communication of medical information using mobile agents," *J. Med. Syst.*, vol. 36, no. 6, pp. 3839–3850, 2012, doi: 10.1007/s10916-012-9857-8.

[25] H. Lee and S. Chang, "RBAC-Matrix-Based EMR Right Management System to Improve HIPAA Compliance," pp. 2981–2992, 2012, doi: 10.1007/s10916-011-9776-0.

[26] N. Shank, E. Willborn, L. Pytlikzillig, and H. Noel, "Electronic health records: Eliciting behavioral health providers' beliefs," *Community Ment. Health J.*, vol. 48, no. 2, pp. 249–254, 2012, doi: 10.1007/s10597-011-9409-6.

[27] Y. Y. Chen, J. C. Lu, and J. K. Jan, "A secure EHR system based on hybrid clouds," *J. Med. Syst.*, vol. 36, no. 5, pp. 3375–3384, 2012, doi: 10.1007/s10916-012-9830-6.

[28] A. M. Ningtyas and I. K. Lubis, "Literatur Review Permasalahan Privasi Pada Rekam Medis Elektronik," *Pseudocode*, vol. 5, no. 2, pp. 12–17, 2018, doi: 10.33369/pseudocode.5.2.12-17.

[29] M. E. Smid and D. K. Branstad, "The Data Encryption Standard: Past and Future," *Proc. IEEE*, vol. 76, no. 5, pp. 550–559, 1988, doi: 10.1109/5.4441.

[30] B. S. Alhaqbani, "Privacy and Trust Management for Electronic Health Records," *Sci. Technol.*, no. June, 2010, [Online]. Available: http://yawlfoundation.org/arthur/students/thesis-Bandar Alhaqbani-No-Sig.pdf.