Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
website: https: //rivierapublishing.id/jii/index.php/
Vol. 4. No. 12. 2025

Electronic Medical Record Security Assessment Using System Security Engineering–Capability Maturity Model (SSE-CMM)

Vira Febriyana*, Imam Sutanto, Hosizah, Arief Ichwani
Universitas Esa Unggul, Indonesia
Email: virafebriyana9@student.esaunggul.ac.id*

Keywords
Security; Electronic Medical Records; SSE-CMM

Abstract
The implementation of Electronic Medical Record (EMR) faces challenges regarding patient information privacy, making it essential to assess the maturity level of its security. This study aimed to conduct an EMR security assessment to evaluate current conditions against those expected to meet the ISO 27002:2022 standard. This qualitative research employed a case study design. Data were analyzed using the System Security Engineering–Capability Maturity Model (SSE-CMM) method and gap analysis. The assessment revealed that the current EMR security level is at the initial/ad hoc stage (level 1), with an average score of 1.06 and a gap of 1.94 from the target defined process level (level 3). Thus, EMR security remains in its early stages, necessitating improvements in formally documented policies and security procedures, which have yet to be implemented.

INTRODUCTION

The advancement of information technology in the era of globalization is now continuing to develop following the need for human activities for ease, speed and high level of accuracy in managing data and information (Muhammad Akbar Al Maruf et al., 2023). In the health sector, this technological advancement encourages the emergence of various innovations (Kröner et al., 2025) which refers to the process of integration and implementation of digital technology to improve and transform services and operations in the health sector (Rachmania et al., 2025). One of these innovations is Electronic Medical Record (EMR) (Maha Wirajaya & Made Umi Kartika Dewi, 2020). Alternatively, EMR is referred to as a computer-based patient record or Electronic Health Record (EHR) (Ge et al., 2025). According to the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records, it is stated that EMR is a medical record made using an electronic system intended for medical providers and currently EMR must be used in all health care facilities in Indonesia (Kementerian Kesehatan Indonesia, 2022). The use of EMR aims to improve the quality of medical services, optimize medical management, strengthen disease detection, prevention and monitoring , and improve data quality (Ge et al., 2025).

However, there are challenges in the use of EMR, namely regarding the privacy of health information (Keshta & Odeh, 2021) which is increasingly a major concern in the health sector (Narayan et al., 2025). A study stated that privacy issues are one of the obstacles in the use of EMR because many still feel worried about their personal information and privacy as users (Huang et al., 2022). Then a study conducted at Riyadh Hospital also reported a similar thing, where only 69.6% had confidence in EMR in protecting patient data from unauthorized access, then as many as 25.5% stated that they had access to EMR without permission which caused significant privacy concerns (Qashqari et al., 2025). Likewise in Indonesia, based on

the findings of a study conducted by Santhi (2025), it is stated that electronic-based health systems have fundamental weaknesses in ensuring data privacy. Existing regulations have not been able to facilitate the development of digital technology, creating a risk of leakage and misuse of medical information (Santhi, 2025). Therefore, it is important to ensure the level of information security in protecting sensitive data, operational continuity and building trust with stakeholders by complying with the aspects of confidentiality, integrity and availability (CIA) (Nugroho & Rochmadi, 2024).

The level of security in EMR can be determined using the System Security Engineering – Capability Maturity Model (SSE-CMM) method. SSE-CMM is a model used to assess and improve an organization's ability to implement security in information technology systems, as well as help understand how far they are capable (Nurbojatmiko et al., 2024). Meanwhile, to meet compliance with the CIA aspect, an information security standard is needed, one of which is standardization and ISO 27002:2022, which is a document that contains requirements and guidelines for implementing information security controls consisting of four clauses, namely organizational, human, physical and technological control clauses (ISO 27002, 2022). In a previous study that described various information security standards, including ISO 27002:2022, it was stated that compliance with these standards can increase trust between patients and healthcare professionals regarding the security and privacy of sensitive information (van der Storm et al., 2023).

Based on the explanation above, it is known that the implementation of EMR must meet the aspects of the CIA in its application both in health care facilities and in health sector institutions that provide EMR practices such as the Health Information Management (HIK) study program at Esa Unggul University, which has an EMR intended for HIK students called EMR "LAB_HIK". This study program produces graduates of a Medical Recorder and Health Information (MRHI) who must have the ability to manage quality medical record services in accordance with the system flow to ensure medical records are available when needed for manual, electronic or hybrid patient services in health facilities in accordance with the Decree of the Minister of Health Number HK.01.01/MENKES/312/2020 concerning Competency Standards for Medical Recorders and Health Information (Kementerian Kesehatan, 2020). The Decree of the Minister of Health encourages the HIK study program to design an EMR system that aims to facilitate HIK students in learning and practicing managing medical record data in electronic form. However, the EMR “LAB_HIK” is currently unknown how secure it is.

Therefore, this study aims to conduct an EMR security assessment using the SSE-CMM method in meeting the ISO 27002:2022 standardization which focuses on technology control clauses and conduct a gap analysis to find out the gap in the current level of security with the expected level so that it can be known which areas must be prioritized for improvement in improving EMR security. Academically, this research contributes to the development of health information security evaluation methodology by integrating the SSE-CMM model and the ISO 27002:2022 standard. Practically, the findings of this study can serve as a reference for the administrators of the "LAB_HIK" EMR and similar educational institutions to identify security vulnerabilities, develop documented security policies, and design structured procedural improvements. Consequently, this research is expected to enhance the maturity level of electronic medical record system security, strengthen patient data protection, and support the

establishment of user trust in health information systems within both educational and clinical service environments.

METHOD

This type of research was qualitative research with a case study design. This research was conducted at the EMR Laboratory of Esa Unggul University Jakarta from September 2024 to February 2025 and has obtained ethical approval by the Ethics Commission of Esa Unggul University with the number: 0924-11.080/DPKE-KEP/FINAL-EA/UEU/XI/2024.

The framework in this study refers to the quality management process, namely plan, do, check, and act (PDCA). PDCA is a continuous cycle for making improvements (Sudirman et al., 2023). This cycle is used because it is in line with procedures for conducting assessments and helps make improvements in increasing the security of EMR.

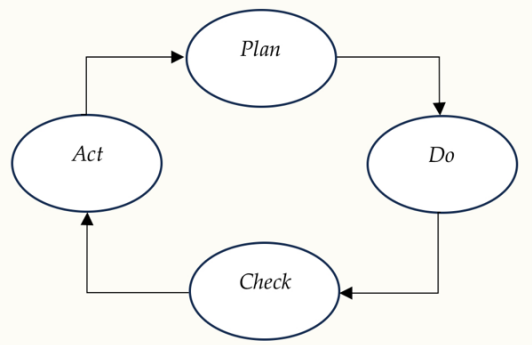

Figure 1. Cycle of PDCA (Ibrahim dan Rusdiana, 2021)

The stages in this study are as follows.

1. Plan, explain the scope and characteristics of EMR and determine ISO 27002:2022 security controls.
2. Do, conduct an EMR security assessment.
3. Check, analyze the results of the EMR security assessment and compare the current security conditions with the expected conditions.
4. Act, provides recommendations on EMR security for improvement by referring to the ISO 27002:2022 standardization guidelines.

Data collection was carried out by reviewing documents and interviewing the EMR design team of the HIK study program. A document review is conducted to review the content of the ISO 27002:2022 document to identify security controls that are appropriate and relevant to the scope and characteristics of the EMR. Meanwhile, interviews were conducted with UI designers, business analysts and programmers to find out the characteristics of the EMR "LAB_HIK" and the security procedures that have been implemented. The interview is also accompanied by a checklist table to obtain EMR safety assessment data. Then the data that has been obtained will be analyzed.

Data analysis was carried out using SSE-CMM and gap analysis methods. The tool used is Ms. Excel to process data and visualize graphs of the results of the EMR security assessment.

1. SSE-CMM, a computational method in measuring the security level of EMR, which has six levels, which are as follows (Riadi & Kurniawan, 2018).

Table 1. Maturity Level Criteria Assessment Index

Level	Range	Desc
0	0 – 0.50	*Non-Existent*
1	0.51 – 1.50	*Initial/Ad-Hoc*
2	1.51 – 2.50	*Repeatable but Infinitive*
3	2.51 – 3.50	*Define Process*
4	3.51 – 4.50	*Managed and Measurable*
5	4.50 – 5.00	*Optimazed*

Source: Adapted from Riadi & Kurniawan (2018)

2. *Gap analysis*, a comparison between the current security conditions of the EMR and the expected conditions (Priadi, 2020) .

$$Q = P - E$$

desc:
Q = *gap*
P = *Current Condition Value*
E = *Expected condition value*

RESULTS AND DISCUSSION

Scope and Characteristics of Electronic Medical Records

The EMR "LAB_HIK" is designed to be website-based and intended for learning activities in accordance with existing standards in managing medical data. This EMR has 12 features and 10 users where each user can only access EMR according to his or her duties and responsibilities, except for admins who can access all EMR features.

Table 2. Features and Users of EMRs"LAB_HIK"

Feature	Function	User
Dashboard	Main page displaying statistics related to visit reports, doctors' schedules and registered system users	All users
Master Data	Database storage	Admin
Registration	Features for registering patients and intended polyclinics	Registration officer and admin
Initial Assessment	Record the patient's initial examination which includes vital signs, anamnesis and whole-body examination	Nurses and admins
Examination	Record the results of the patient's examination	Doctors and admins
Counseling	Features for student mental health screening and monitoring	Psychologist and admin
Laboratory	Record the patient's laboratory examination according to the doctor's request	Laboratory staff and admin
Radiologi	Record the patient's radiological examination according to the doctor's request	Radiology and admin
Coding	Record clinical codifications and actions according to the results of the patient's examination	Medical records and admin
Pharmacy	For pharmacists to perform patient medicine services	Pharmacists and admins

Feature	Function	User
Cashier	Processing payments according to the type of payment and the patient's treatment	Cashier and admin
Reporting	Provide reports related to patient visits, top 10 diseases, top 10 actions, payments, supporting examinations, medications and referrals	All users

Source: Internal Documentation of EMR "LAB_HIK" Design Team

However, this EMR still has shortcomings that have not been implemented stably and security procedures are still limited. The completeness of the features in the EMR "LAB_HIK" is intended to expand its use, namely at the Esa Medhika Clinic at Esa Unggul University, but further development is still needed.

Electronic Medical Record Security Assessment

The EMR security maturity assessment focuses on the ISO 27002:2022 technology control clause with the selection of controls that have been adapted to the scope and characteristics of the EMR "LAB_HIK". The assessment data was analyzed based on 41 statements from 15 controls used. The controls with the largest averages are in privileged access control, access control to code source, logging control, cryptographic usage control, secure development cycle control and secure coding control by 2. Meanwhile, the smallest average value of 0 was found in malware protection controls, data leak prevention controls, information backup controls, network security controls, network service controls and network separation controls. Overall, the results of the EMR security maturity level "LAB_HIK" are currently at level 1 or Initial/Ad hoc with a value of 1.06 with the expected condition being level 3 or define process. The gap between the current security condition and the expectation condition is 1.94, where there is still a considerable gap. The results of the assessment can be seen in the following table.

Table 3. Results of Electronic Medical Record Security Assessment

Security Controls	Maturity Level		Gap
	Actual Condition	Expectation Conditions	
8.2 Privileged access rights	2	3	1
8.3 Restrictions on access to information	1,5	3	1,5
8.4 Access to code sources	2	3	1
8.5 Secure authentication	1	3	2
8.7 Protection against *malware*	0	3	3
8.11 *Masking data*	1,33	3	1,67
8.12 Data leak prevention	0	3	3
8.13 Backup information	0	3	3
8.15 Creating *logs*	2	3	1
8.20 Network security	0	3	3
8.21 Network service security	0	3	3
8.22 Network separation	0	3	3
8.24 Use of cryptography	2	3	1
8.25 Secure development cycle	2	3	1
8.26 Secure coding	2	3	1
Average	1,06	3	1,94

Source: Data analysis based on interviews and document review (2024-2025)

An image contains diagrams, lines, text AI-generated content may be wrong.gap analysis It is known that priority areas for improvement in security procedures are malware protection controls, data leakage prevention controls, information backup controls, network security controls, network service controls, and network separation controls. The magnitude of the gap between current and desired conditions is illustrated as follows.

(Tanuwijaya, 2022);(Haqqi et al., 2022) maturity level The security score of PT. XYZ's Sipeter is 1.55, indicating that security is inconsistent and security controls are carried out informally, meaning there are no policies or standard guidelines and they are not well documented. Therefore, to achieve the expected security conditions at EMR "LAB_HIK" Improvements are needed in security policies and procedures that comply with standards to improve EMR security to a more mature and stable level. Previous studies have shown that if an organization has implemented security that complies with existing agreements and standards, as well as formally documented procedures, then (Tanuwijaya, 2022) maturity level will be higher. (Haqqi et al., 2022)

Formal, documented policies such as Standard Operating Procedures (SPOs) can be created simply and developed as the EMR is implemented. This policy serves to clarify and ensure that security procedures have been carried out in accordance with the principles, standards and objectives in managing the security of EMR, helping to comply with existing standards and regulations, and ensuring compliance of its users. Meanwhile, security procedures that have not been implemented can be carried out in stages following the ability to improve the safety of the EMR in accordance with the ISO 27002:2022 standard so that it can reach the desired level of defining process.

CONCLUSION

The safety of the HIK study program is currently at the initial/ad hoc level with an average value of 1.06 with a gap of 1.94 from the expected condition, namely the level of the define process in complying with the ISO 27002:2022 standard. Security improvements and improvements include formally documented policy aspects and the implementation of security procedures in accordance with ISO 27002:2022 standards. There are limitations in this research, where the assessment carried out only focuses on technology clauses in assessing the safety of EMR. Therefore, for further research, it can be expected to add organizational, human, and physical control clauses to the ISO 27002:2022 standard in assessing the safety of EMR and combining these standards with other safety standards. However, our research can be used as a reference in understanding the EMR security assessment process.

REFERENCES

Ge, D., Xia, Y., & Zhang, Z. (2025). Analyzing the Medical Record Homepages Quality in a Chinese EMR System. *BMC Medical Informatics and Decision Making*, *25*(1). https://doi.org/10.1186/s12911-025-02949-1

Haqqi, D. P., Ghozali, K., & Ginardi, R. V. H. (2022). Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 dengan Menggunakan Model SSE-CMM (System Security Engineering Capability Maturity Model) pada Perusahaan

Daerah Air Minum Surya Sembada Kota Surabaya. *Jurnal Teknik ITS*. http://ejurnal.its.ac.id/index.php/teknik/article/download/91532/7126

Huang, J., Pang, W. S., Wong, Y. Y., Mak, F. Y., Chan, F. S. W., Cheung, C. S. K., Wong, W. N., Cheung, N. T., & Wong, M. C. S. (2022). Factors Associated With the Acceptance of an eHealth App for Electronic Health Record Sharing System: Population-Based Study. *Journal of Medical Internet Research*, *24*(12). https://doi.org/10.2196/40370

Ibrahim, H. T., & Rusdiana, H. A. (2021). *Manajemen Mutu Terpadu* (Vol. 1). YRAMA WIDYA. http://www.yrama-widya.co.id

ISO 27002. (2022). *Information Security, Cybersecurity and Privacy Protection-Information Security Controls*.

Kementerian Kesehatan. (2020). *Keputusan Menteri Kesehatan Nomor HK.01.07/MENKES/312/2020 Tentang Standar Profesi Perekam Medis dan Informasi Kesehatan*.

Kementerian Kesehatan Indonesia. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis*. https://yankes.kemkes.go.id/unduhan/fileunduhan_1662611251_882318.pdf

Keshta, I., & Odeh, A. (2021). Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Kröner, S., Schreiweis, B., Strotbaum, V., Brandl, L. C., Pobiruchin, M., & Wiesner, M. (2025). Consumer Perspectives on the National Electronic Health Record and Barriers to its Adoption in Germany: Does Health Policy Require a Change in Communication? *BMC Health Services Research*, *25*(1). https://doi.org/10.1186/s12913-024-12175-6

Maha Wirajaya, M. K., & Made Umi Kartika Dewi, N. (2020). Analisis Kesiapan Rumah Sakit Dharma Kerti Tabanan Menerapkan Rekam Medis Elektronik. *Jurnal Kesehatan Vokasional*, *5*(1), 1–9. https://doi.org/10.22146/jkesvo.53017

Muhammad Akbar Al Maruf, Darman, & Zila Razilu. (2023). Rancang Bangun Manajemen Bandwidth Jaringan Pada Laboratorium Teknik Komputer dan Jaringan. *Decode: Jurnal Pendidikan Teknologi Informasi*, *3*(2), 246–256. https://doi.org/10.51454/decode.v3i2.177

Narayan, S. M., Kohli, N., & Martin, M. M. (2025). Addressing Contemporary Threats in Anonymised Healthcare Data Using Privacy Engineering. *Npj Digital Medicine*, *8*(1). https://doi.org/10.1038/s41746-025-01520-6

Nugroho, S., & Rochmadi, T. (2024). Analysis of Information Security Readiness Using the Index KAMI. *Decode: Jurnal Pendidikan Teknologi Informasi*, *4*(3), 881–886. https://doi.org/10.51454/decode.v4i3.602

Nurbojatmiko, Aini, Q., Wasiqi, N. C., Alfajri, M. F., Ulinnuha, Z., Purwati, Y. K., Ayu, I. K., & Yasmin, N. A. (2024). Risk Assessment Maturity Level of Academic Information System Using ISO 27001 System Security Engineering-Capability Maturity Model. *Journal of Applied Engineering and Technological Science (JAETS)*, *5*(2), 941–954. https://doi.org/10.37385/jaets.v5i2.2971

Priadi, A. A. (2020). *Penelitian Terapan Bidang Pelayaran dengan Metode Gap Analysis* (A. Maryati & R. Hariyanti, Eds.; 1st ed., Vol. 1). Politeknik Ilmu Pelayaran Semarang. https://repository.pip-semarang.ac.id/3884/1/gap%20analysis.pdf

Qashqari, A. A., Almutairi, D. S., Ennaceur, S. A., Farhah, N. S., & Almohaithef, M. A. (2025). Healthcare Professionals' Perceptions of Electronic Medical Record Privacy and Its Impact on Work Quality in Riyadh Hospitals. *Saudi Medical Journal*, *46*(3), 299–306. https://doi.org/10.15537/smj.2025.46.3.20240928

Rachmania, I. N., Yudoko, G., Basri, M. H., & Setyaningsih, S. (2025). Understanding Patient Perception of Digital Value Co-Creation in Electronic Health Record Through Clustering Approach. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-91287-3

Riadi, I., & Kurniawan, E. (2018). Security Level Analysis of Academy Information Systems Based On Standard ISO 27002:2003 Using SSE-CMM. *International Journal of Computer Science and Information Security*, *16*(1), 139–147. https://doi.org/10.13140/RG.2.2.20925.15840

Santhi, N. N. P. P. (2025). Patient Data Privacy Challenges in Electronic Health Systems: A Juridical Analysis of Medical Information Protection in Indonesia. *West Science Law and Human Rights*, *3*(1), 1–8. https://doi.org/https://doi.org/10.58812/wslhr.v3i01.1577

Sudirman, Yanuarti, R., Oktarianita, Fajrini, F., & Widihastuti, S. K. (2023). *Manajemen Mutu Pelayanan Kesehatan*. Ara Digital Mandiri.

Sugiyono. (2022). *Metode Penelitian Kualitatif*. Alfabeta Bandung.

Tanuwijaya, H. (2022). Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002. *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *11*(3), 571–582. https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/article/view/993

van der Storm, S. L., Jansen, M., Meijer, H. A. W., Barsom, E. Z., & Schijven, M. P. (2023). Apps in Healthcare and Medical Research; European Legislation and Practical Tips Every Healthcare Provider Should Know. *International Journal of Medical Informatics*, *177*, 105141. https://doi.org/10.1016/j.ijmedinf.2023.105141