

DOI: <https://doi.org/10.38035/systemic.v2i1><https://creativecommons.org/licenses/by/4.0/>

Analysis of the Security and Confidentiality of Electronic Medical Records in Supporting Healthcare Service Quality at Bhayangkara Level I Hospital, PUSDOKKES POLRI

Nanang Ari Widiyanto¹, Irda Sari²

¹Politeknik Piksi Ganesha, Bandung, Indonesia, Widiyantonanangari@gmail.com

²Politeknik Piksi Ganesha, Bandung, Indonesia, Irdasari13@gmail.com

Corresponding Author: Widiyantonanangari@gmail.com¹

Abstract: The development of Electronic Medical Records (EMRs) contributes to improving healthcare service quality by facilitating access to information, accelerating service delivery, and increasing data accuracy. However, implementation continues to face challenges related to data security, patient-information confidentiality, and suboptimal user compliance with standard operating procedures. This study aimed to analyze the implementation of EMR security and confidentiality in supporting healthcare service quality at Bhayangkara Level I Hospital, Puskokkes Polri. A descriptive qualitative approach was employed using observation, interviews, questionnaires as a supporting instrument, and document review. The findings showed that the EMR system had implemented several security mechanisms, including username-and-password authentication, role-based access restrictions, audit trails, and periodic data backup and recovery. Data confidentiality was maintained by restricting access to authorized healthcare personnel. Nevertheless, challenges remained in user behavior and compliance with established policies. Appropriate implementation of security and confidentiality measures can increase patient trust, accelerate service processes, and maintain the integrity of medical data. Continuous supervision, training, and system evaluation are therefore required to further improve healthcare service quality.

Keyword: Security, Confidentiality, Electronic Medical Records, Healthcare Service Quality.

INTRODUCTION

The development of information technology in healthcare has brought significant changes to service systems, particularly in patient-data management. The transition from paper-based medical records to Electronic Medical Records (EMRs) enables data to be stored, processed, and accessed more rapidly and accurately and facilitates integration across service units. This is consistent with the policy of the Indonesian Ministry of Health, which emphasizes that EMRs are intended to improve service quality through the utilization of information technology (Ministry of Health of the Republic of Indonesia, 2020).

EMR implementation not only improves the efficiency of healthcare professionals but also supports more accurate, data-driven clinical decision-making. An integrated system enables real-time access to patient information, thereby accelerating diagnostic and medical-

treatment processes. However, alongside these benefits, EMR implementation also creates challenges, particularly in relation to the security and confidentiality of patient data.

Medical records contain sensitive information, including patient identity, medical history, examination results, and medical procedures. Inadequate management may result in data leakage and privacy violations. Protecting patient data in electronic systems is therefore essential for maintaining public trust in healthcare services (Pratama & Sari, 2022). Data security in EMR systems is also an important factor in ensuring continuity and quality of healthcare services (Nugroho & Wibowo, 2021).

Data security encompasses physical and system protection, including authentication, encryption, audit trails, and data-backup mechanisms (Hidayat et al., 2021). Confidentiality, meanwhile, concerns restrictions on access rights, professional ethics, and regulatory compliance (Wahyuni et al., 2021). Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 emphasizes that medical records are confidential and may only be accessed by authorized parties (Ministry of Health of the Republic of Indonesia, 2022).

Various studies have shown that the security and confidentiality of EMR data remain challenging. Weaknesses in access control and risk management have been identified in healthcare facilities (Sari & Handayani, 2020; Saputra & Firmansyah, 2020). Information-system security also plays an important role in protecting patient confidentiality (Yari et al., 2021). More recent evaluations have identified gaps in the implementation of security policies and low compliance with standard operating procedures (Putri & Kurniawan, 2023; Kurniawati & Santoso, 2022). Personal-data protection in digital systems has therefore become increasingly important in the era of healthcare transformation (Lestari & Utami, 2023).

Bhayangkara Level I Hospital, Puskokkes Polri, as a central referral hospital, has implemented EMRs to improve healthcare service quality. Nevertheless, several challenges remain, including human-resource readiness, limitations in technological infrastructure, and suboptimal compliance with established procedures.

Data security and confidentiality play an important role in improving healthcare service quality. A secure system can increase patient trust, accelerate access to information, and maintain the accuracy of medical data. Conversely, system weaknesses may contribute to service errors that could potentially compromise patient safety.

Based on these considerations, this study aimed to analyze the implementation of Electronic Medical Record security and confidentiality in supporting healthcare service quality at Bhayangkara Level I Hospital, Puskokkes Polri. The study is expected to provide an overview of current conditions and serve as a basis for recommendations to improve the quality of EMR management.

METHOD

This study used a descriptive research method with a qualitative approach to obtain an in-depth understanding of the implementation of EMR security and confidentiality and their relationship with healthcare service quality. This approach was selected to enable comprehensive exploration of actual field conditions through direct interaction with informants.

A cross-sectional design was used, in which data were collected during a defined period without any specific intervention applied to the research object. This design was selected because it provides a snapshot of the current implementation of EMR security and confidentiality in the hospital.

The study was conducted at Bhayangkara Level I Hospital, Puskokkes Polri, from 1 to 30 June 2026. The hospital was selected because it had implemented an Electronic Medical Record system in healthcare delivery. Research participants consisted of interview informants and questionnaire respondents. Informants were selected using purposive sampling based on

specific criteria, namely active use of the EMR system and an understanding of data-security and confidentiality procedures.

Data were collected through observation, in-depth interviews, questionnaires, and document review. Observation was used to examine the implementation of security procedures directly; interviews were used to obtain information based on informants' experiences and understanding; and document review was used to support and verify information obtained from observations and interviews. Data trustworthiness was maintained through source and technique triangulation by comparing information obtained from different sources and data-collection methods (Sugiyono, 2023; Notoatmodjo, 2018).

The study primarily used qualitative data obtained directly from informants. Structured interviews and a questionnaire were also used as supporting instruments to provide a general description of security, confidentiality, and healthcare service quality. Primary data were obtained from interviews and questionnaires, while secondary data were obtained from supporting documents such as Standard Operating Procedures (SOPs) and hospital policies.

Data collection techniques included the following:

Questionnaire

A questionnaire using a Likert scale was used to measure respondents' perceptions of EMR security and confidentiality and healthcare service quality. The questionnaire involved 30 respondents.

Structured Interviews

Structured interviews were conducted with five informants: the Head of the Medical Records Unit, a registration medical records officer, a physician, a nurse, and a SIMRS officer. The interviews explored system policies, implementation, and supervision.

Table 1. Characteristics of Informants

No.	Informant	Position	Length of Service
1	Informant 1	Head of the Medical Records Unit	5 years
2	Informant 2	Registration Medical Records Officer	3 years
3	Informant 3	Physician	5 years
4	Informant 4	Nurse	2 years
5	Informant 5	SIMRS Officer	3 years

Direct Observation

Direct observation was conducted to examine the implementation of user login, access-right restrictions, audit trails, and security procedures operating in the hospital.

Document Review

Document review included SOPs, regulations, and other supporting documents related to EMR security and confidentiality.

These data-collection methods were expected to provide a comprehensive description of the implementation of EMR security and confidentiality and their role in supporting healthcare service quality.

RESULTS AND DISCUSSION

Result

Based on the interviews, the study identified the implementation of security and confidentiality mechanisms within the EMR system at Bhayangkara Level I Hospital, Puskokkes Polri. The data were obtained from personnel directly involved in using the EMR system.

The findings are presented descriptively to describe the current system, including user authentication, data integrity and audit trails, system availability, and security evaluation.

The EMR system uses username-and-password authentication. Each user has a personal account and accesses the system according to their assigned authority. Access rights are configured according to position and work unit, thereby limiting access to patient data to authorized personnel.

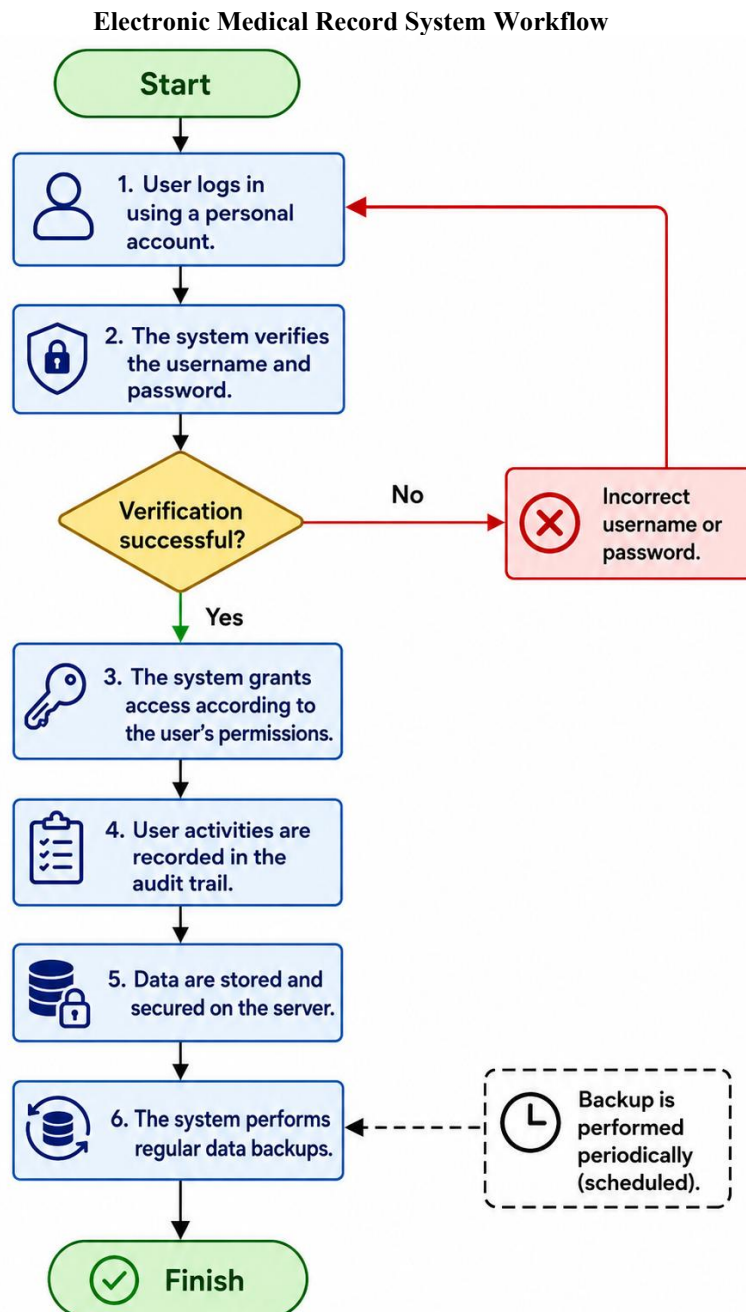
The system is also equipped with an audit-trail feature that records user activity. Historical data changes can only be accessed by specific authorized personnel. Access restrictions and user controls are applied to prevent unauthorized modification of data.

To maintain system availability, server maintenance is conducted periodically and security mechanisms such as firewalls are used. System disruptions are reported to occur infrequently, and data backup and recovery procedures are available. Nevertheless, challenges remain in preventing unauthorized access and ensuring user compliance with applicable security policies.

Table 2. Summary of Informant Interview Findings

No.	Assessed Aspect	Interview Finding	Implementation Status
1	User login system	Uses username and password	Implemented
2	Account ownership	Each user has a personal account	Implemented
3	Access rights	Based on position and work unit	Implemented
4	Audit trail	Available and records user activities	Implemented
5	Access to data history	Restricted to authorized personnel	Implemented
6	Prevention of data modification	System access restrictions are applied	Implemented
7	System availability	Maintained through server maintenance	Implemented
8	System disruptions	Rarely occur	Implemented
9	Backup and recovery	Performed periodically	Implemented
10	Challenges	Unauthorized access and user compliance	Requires continued attention

The interview findings indicate that the EMR login system uses usernames and passwords and that each user has a personal account. Access rights are assigned based on position and work unit, while user activities are recorded through an audit trail. Access to historical data is limited to authorized personnel, and changes to data are restricted according to assigned permissions. System availability is maintained through server maintenance, and backup and recovery are performed periodically. However, risks related to unauthorized access and user compliance with security procedures remain.



The workflow demonstrates that the EMR system applies security processes beginning with user authentication and continuing through data storage. Each user activity is recorded as part of system monitoring, while secure storage and periodic backups are performed to maintain data security and availability.

Questionnaire data were analyzed using a Likert scale to determine respondents' assessments of the Electronic Medical Record system. The results are presented below.

Table 3. Summary of Questionnaire Results

No.	Statement	STS (1)	TS (2)	N (3)	S (4)	SS (5)	Total Score	Mean	Category
1	The EMR system is easy to use	0	2	5	15	8	119	3.96	Good

2	Patient data can be accessed quickly	1	3	6	14	6	111	3.70	Good
3	Users experience obstacles when using the system	2	5	8	10	5	101	3.36	Fair
4	EMR accelerates patient services	0	1	4	16	9	123	4.10	Good
5	Medical information is accurate	0	2	6	15	7	117	3.90	Good
6	Patient data are complete	1	4	7	13	5	107	3.56	Good
7	EMR reduces service errors	0	2	5	17	6	117	3.90	Good
8	The system rarely experiences disruptions	3	6	9	8	4	94	3.13	Fair
9	Patient-data security is maintained	2	5	7	11	5	102	3.40	Fair

Note: Total Score = (STS×1) + (TS×2) + (N×3) + (S×4) + (SS×5). Mean = Total Score ÷ Number of Respondents.

Assessment categories: 1.00-1.80 = Very Poor; 1.81-2.60 = Poor; 2.61-3.40 = Fair; 3.41-4.20 = Good; 4.21-5.00 = Very Good.

Based on the questionnaire results, most indicators were categorized as good, indicating that the EMR system was generally effective in supporting healthcare services. The highest score was obtained for accelerated patient services (mean 4.10), followed by ease of use (3.96) and medical-information accuracy (3.90), indicating that the system contributes to greater efficiency and improved performance among healthcare personnel.

However, several indicators remained in the fair category, including obstacles encountered during system use (3.36), system disruptions (3.13), and patient-data security (3.40). These findings indicate that technical barriers such as network disruptions and non-technical factors such as human error arising from shared or alternating account use remain present.

Across the nine assessed aspects, six were categorized as good and three as fair. Overall, EMR implementation has supported service processes, particularly in ease of system use, speed of patient-data access, acceleration of service delivery, accuracy of medical information, data completeness, and reduction of service errors. Nevertheless, obstacles in system use, system disruptions, and patient-data security require further attention and improvement. Continuous evaluation and corrective action are therefore necessary to optimize system utilization.

Discussion

Based on the questionnaire and interview findings, EMR security at the hospital has generally been implemented appropriately. This is reflected in the predominance of questionnaire assessments in the good category and is supported by interview findings indicating that the system has implemented basic security mechanisms such as user authentication, access-right management, audit trails, and data backup and recovery.

In terms of system effectiveness, the EMR was rated as capable of accelerating patient services, with the highest mean score of 4.10. Ease of use (3.96) and medical-information accuracy (3.90) also indicate that the system assists healthcare professionals in improving work efficiency and accuracy. These benefits are supported by personal accounts and position-based access rights, ensuring that users can access only the data for which they are authorized.

From a security perspective, the system is equipped with an audit trail that records user activities and access restrictions designed to prevent unauthorized data modification. System availability is maintained through periodic server maintenance, firewall use, and data backup and recovery. These measures indicate that the system has established important mechanisms for protecting medical data.

Nevertheless, several indicators remained in the fair category, including obstacles during system use (mean 3.36), system disruptions (3.13), and patient-data security (3.40). These findings demonstrate that challenges remain in EMR implementation. Technically, network disruptions can cause the system to become slow or difficult to access. From a non-technical perspective, human error was identified in the form of users sharing or alternating accounts with colleagues.

Such practices may reduce system security because they can facilitate misuse of access privileges and decrease the accuracy and accountability of audit-trail records. Patient-data completeness also requires continued improvement to support more optimal service delivery.

Accordingly, improvements are needed in several areas, including network infrastructure, system security, and enforcement of discipline in the use of personal accounts. Periodic socialization and training should also be conducted so that all users understand the importance of protecting the security and confidentiality of patient data.

Overall, the EMR system has had a positive impact on healthcare service quality. However, further optimization is required, particularly in system stability, data security, and user compliance, so that the system can operate more securely and effectively.

CONCLUSION AND RECOMMENDATIONS

Conclusion

The implementation of EMR security and confidentiality at Bhayangkara Level I Hospital, Puskokkes Polri, plays an important role in improving healthcare service quality. Security measures have been implemented through physical safeguards, including restricted access to server rooms, as well as system safeguards such as passwords, data encryption, audit trails, and periodic data backups to prevent unauthorized access and data loss. Confidentiality is maintained by restricting access to authorized healthcare professionals and applying relevant regulations. A secure system that protects data confidentiality contributes positively to healthcare quality because patient information can be accessed rapidly, accurately, and consistently, thereby supporting appropriate clinical decision-making. Nevertheless, several implementation challenges remain, including limited awareness among human resources regarding account security, infrastructure limitations, and suboptimal implementation of SOPs. Continuous training, supervision, and system evaluation are therefore required to optimize EMR security and confidentiality and sustain improvements in healthcare service quality.

Recommendations

Bhayangkara Level I Hospital, Puskokkes Polri, is encouraged to continue improving EMR implementation, particularly in relation to patient-data security and confidentiality, in accordance with applicable SOP standards. The hospital should strengthen supervision of system use and ensure that all healthcare personnel use the system only within their assigned authority, including a strict prohibition on sharing usernames and passwords. The SIMRS unit should strengthen system security through improved encryption, more effective user-access management, and periodic server maintenance to maintain system stability. Technological infrastructure should also be improved by updating computers and systems to more recent versions so that EMR performance becomes faster, more secure, and more efficient. In addition, periodic training and socialization should be provided to all users to improve understanding of the importance of protecting patient-data security and confidentiality. Future researchers are encouraged to expand this study by incorporating additional variables or alternative methods to obtain a more comprehensive understanding of EMR implementation.

REFERENCES

- Hidayat, T., & Prasetyo, E. (2021). Analisis keamanan sistem informasi rekam medis elektronik menggunakan metode ISO 27001. *Jurnal Teknologi Informasi dan Kesehatan*, 8(2), 100-108.
- Kementerian Kesehatan Republik Indonesia. (2020). Pedoman penyelenggaraan rekam medis elektronik di fasilitas pelayanan kesehatan. Jakarta: Kementerian Kesehatan RI.
- Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang rekam medis. Jakarta: Kementerian Kesehatan RI.
- Kurniawati, D., & Santoso, B. (2022). Evaluasi penerapan keamanan data pasien pada sistem informasi kesehatan berbasis digital. *Jurnal Ilmu Kesehatan*, 11(1), 55-63.
- Lestari, R., & Utami, S. (2023). Implementasi perlindungan data pribadi pada sistem rekam medis elektronik di era digital. *Jurnal Kesehatan Digital*, 5(1), 25-33.
- Nugroho, A., & Wibowo, T. (2021). Implementasi keamanan data pada sistem rekam medis elektronik di rumah sakit. *Jurnal Manajemen Informasi Kesehatan Indonesia*, 9(1), 1-8.
- Pratama, R., & Sari, M. (2022). Perlindungan data pasien dalam sistem informasi kesehatan berbasis elektronik. *Jurnal Kesehatan Masyarakat*, 10(3), 210-218.
- Putri, N. A., & Kurniawan, H. (2023). Evaluasi keamanan dan kerahasiaan data pasien pada sistem rekam medis elektronik. *Jurnal Informatika Kesehatan Indonesia*, 11(1), 15-23.
- Salsabila, K., & Sari, I. (2026). Analisis Sistem Informasi Rekam Medis Elektronik Terhadap Efisiensi Waktu Pelayanan di Unit Pendaftaran Rawat Jalan Rumah Sakit X. *Journal of Medical Record Student (JMeRS)*, 4(1).
- Saputra, A., & Firmansyah, R. (2020). Analisis risiko keamanan informasi pada sistem rekam medis elektronik. *Jurnal Sistem Informasi*, 6(2), 75-83.
- Sari, D. P., & Handayani, L. (2020). Analisis penerapan keamanan informasi pada rekam medis elektronik di rumah sakit. *Jurnal Rekam Medis dan Informasi Kesehatan*, 3(2), 85-92.
- Sari, I. (2021). Keamanan Data pada Sistem Rekam Medis Elektronik di Rumah Sakit. *Jurnal Informatika Kesehatan Indonesia*, 6(1), 1-8.
- Sari, I., & Syahputra, A. K. (2023). Analisis Implementasi Rekam Medis Elektronik di Rumah Sakit Radjak Hospital Group. *EDU RMIK Jurnal Edukasi Rekam Medis dan Informasi Kesehatan*.
- Wahyuni, S., & Rahmawati, N. (2021). Penerapan keamanan informasi dalam menjaga kerahasiaan data pasien di rumah sakit. *Jurnal Administrasi Kesehatan*, 9(2), 120-128.
- Yari, A., Rahman, F., & Putra, D. (2021). Keamanan sistem informasi kesehatan dalam menjaga kerahasiaan data pasien. *Jurnal Sistem Informasi Kesehatan*, 7(2), 45-52.