INDONESIAN JOURNAL OF HEALTH INFORMATICS

ORIGINAL RESEARCH

Review of Medical Record Data and Information Security in the Medifirst application at Bakti Pajajaran Regional Hospital

Furqon Sabiq Husaini[1*], Laela Indawati [2]

[1,2] Department of Medical Record and Health Information, Faculty of Health Sciences, Universitas Esa Unggul, Jakarta, Indonesia

* Correspondence to:
Furqon Sabiq Husaini
Department of Medical Record and Health Information, Faculty of Health Sciences, Universitas Esa Unggul, Jakarta, Indonesia
Email: sabiqfurqon@student.esaunggul.ac.id

Received: 16-07-2026
Accepted: 12-08-2026
Published: 13-08-2026

Citation:
Husaini, F. S., & Indawati, L. (2026). Review of Medical Record Data and Information Security in the Medifirst application at Bakti Pajajaran Regional Hospital. Indonesian Journal of Health Informatics.

Abstract

Objective: This study aims to identify the data and information security of medical records in the MediFirst application at Bakti Pajajaran Regional General Hospital (RSUD Bakti Pajajaran) based on three key factors: confidentiality, integrity, and availability.

Methods: This research employed a descriptive qualitative method, utilizing observations and interviews analyzed qualitatively to provide a direct overview of data security within the MediFirst application at RSUD Bakti Pajajaran. The study was conducted at Bakti Pajajaran Regional General Hospital, located at Jl. KSR Dadi Kusmayadi No. 27, Cibinong District, Bogor Regency, West Java 16914, on October 5, 2024. The study included 8 informants: 5 medical record staff members, 2 IT officers, and 1 head of the medical records department.

Results: Based on the findings at RSUD Bakti Pajajaran, the MediFirst application has implemented various data and information security mechanisms covering confidentiality, integrity, and availability. In terms of confidentiality, the system uses data encryption with the Advanced Encryption Standard (AES) algorithm to protect patient data and implements access control through individual usernames and passwords based on Role-Based Access Control (RBAC). Additionally, biometric systems, Virtual Private Networks (VPNs), and Non-Disclosure Agreements (NDAs) are utilized to prevent unauthorized access and maintain patient privacy. Regarding integrity, the MediFirst application utilizes audit logs, hash functions, and digital signatures to ensure data remains accurate and unaltered without authorization. Audit trails are used to transparently monitor user activities, while system updates and security patches are applied periodically after evaluation and testing phases. Regarding availability, the hospital has implemented routine data backups, redundancy and failover systems, and periodic monitoring to maintain application stability and ensure medical record data remains accessible when needed. Overall, the security measures in the MediFirst application effectively support medical record protection, though further developments, such as implementing two-factor authentication, are still required to enhance system security.

Conclusions: In terms of confidentiality, the MediFirst application utilizes individual authentication mechanisms (usernames and passwords) for each user, restricting medical record access based on respective personnel authority. The system also records login activities

for oversight and internal audit support. Regarding integrity, the application successfully maintains the accuracy and completeness of medical records through access restrictions and user activity logging, minimizing the risk of unauthorized data alterations. For availability, the MediFirst system adequately supports service operations by allowing authorized personnel to access medical records as needed. System maintenance and IT support actively help maintain availability, although potential technical disruptions and network dependency remain challenges that require ongoing attention.

Keywords: Review, Data security, MediFirst app.

Background

Today, the massive use of information technology has reached many sectors, including healthcare. Technology in the healthcare sector offers numerous benefits. Among the advantages gained is accurate and comprehensive patient health information, which enables providers to deliver the best possible care (Cholik, 2021). These various advantages encourage the sector to adopt information technology to provide high-quality healthcare services, such as in hospitals.

Hospitals are healthcare facilities that provide medical services to individuals through promotive, preventive, curative, rehabilitative, and palliative care. They also provide inpatient, outpatient, and emergency services (Kemenkes, 2023). To provide excellent service, hospitals are obligated to maintain medical records (Kemenkes, 2022).

Medical record keeping involves the provision of documents containing patient identity, examinations, actions, treatments, and services that have been provided to the patient. The development of information and communication technology has significantly influenced changes in medical record management, shifting towards a worldwide healthcare trend: electronic medical records (EMR). Electronic medical records are created using electronic systems intended for medical record administration (Kemenkes, 2022). To enable EMR management tasks—such as data storage and the ability to generate accurate data to reduce unwanted errors—it is necessary to utilize a Hospital Management Information System (Annisa & Tria, 2020).

A Hospital Management Information System (HMIS / SIMRS) is an integrated user-machine system that utilizes computer hardware and software, as well as manual procedures such as analytical models, supervision planning, decision-making, and databases. The hospital management information system also provides information to support management operations and decision-making functions within the system's organization (Annisa & Tria, 2020).

A high-quality system is one that aligns with and meets established standards. To prevent the rejection of a developed system, its quality must be well-maintained. System quality can be measured through indicators, which include system security (Sugandi & Halim, 2020).

System security is intended to protect information from unauthorized parties and includes access control elements, meaning that access rights can be restricted by regulating who is authorized to access the system and who is not. One issue regarding information system security principles is when users continuously exchange data by sharing the same username and password. Furthermore, many people widely share identical usernames and passwords. This contradicts the access control aspect, which focuses on regulating information access restrictions. If an input error occurs that complicates the identification process, it will undoubtedly have fatal consequences. There are concerns that it will lead to the misuse of information if this practice continues (Rabia & Dety Mulyanti, 2023).

Based on previous research conducted by Puguh Ika Listyorini and Intan Sintya, data security and confidentiality have currently become a crucial and continuously evolving issue. Efforts must be made to keep the system safe from various threats that could disrupt its smooth operation. In some cases,

data security has evolved into a task requiring substantial handling and safeguarding costs. Due to the numerous crimes of patient data theft occurring in hospitals, it can be concluded that patient data security is at risk (Listyorini & Sintya, 2021).
Subsequent research by Muh Amin highlights that the confidentiality of electronic medical record usage must be carefully managed, particularly regarding access rights with usernames and passwords for logging in and out, as well as EMR security risks (Amin et al., 2021). Data security involves measures against information theft or leakage (Herisasono, 2024).
This research was conducted at Bakti Pajajaran Regional General Hospital (RSUD Bakti Pajajaran), a Type B teaching and regional referral hospital owned by the Bogor Regency regional government. Established in 1982 and located in the government center of Bogor Regency, it was previously known as Cibinong Regional General Hospital. As of May 27, 2025, the hospital officially changed its name. In accordance with the Bogor Regent's Decree No. 445/338/kpts/huk/2009, RSUD Bakti Pajajaran was designated as a Regional Work Unit (SKPD) implementing the Regional Public Service Agency financial management pattern (PPK-BLUD), with the hope of improving its performance in serving the community. RSUD Bakti Pajajaran has a capacity of 515 beds, and its outpatient installation features 34 clinics.
Based on initial observations, HMIS login users have not yet utilized two-factor authentication (2FA) because the system still requires further development. Furthermore, the database in the MediFirst system is not yet fully encrypted, meaning data security aspects remain sub-optimal. Electronic medical record users at RSUD Bakti Pajajaran implement three principles of data and information security, known as Confidentiality, Integrity, and Availability (CIA Triad).

Research Methods

This research employed a descriptive qualitative method, utilizing observations and interviews analyzed qualitatively. The objective was to provide a comprehensive overview and directly observe data security within the MediFirst application at Bakti Pajajaran Regional General Hospital (RSUD Bakti Pajajaran). The study was conducted at Bakti Pajajaran Regional General Hospital, located at Jl. KSR Dadi Kusmayadi No. 27, Cibinong District, Bogor Regency, West Java 16914, on October 5, 2024. There were 8 informants in this study, comprising 5 medical record staff members, 2 IT officers, and 1 head of the medical records department.
The primary focus of this research was to analyze the application's security features, such as data encryption and user access control, as well as to evaluate its compliance with national personal data protection regulations. Additionally, the study aimed to identify system errors and examine how the data backup and recovery processes are executed. The results of this research are expected to provide recommendations on how to optimize the use of the MediFirst application to enhance the security of medical record data.

Result and Discussion

Identifying the security of medical record data and information in terms of confidentiality factors *(Confidentiality)*

Table 1 Implementation of Confidentiality

Theme	Category	Coding
Implementation of Confidentiality *(Confidentiality)*	Encryption	Unreadable format using keys
		Protecting patient data between servers
		Using algorithms
		Using AES (Advanced Encryption Standard)
		Using encryption

		Protecting sensitive data
		Data conversion process
	Confidentiality Access Control	Already using a biometric system
		Login with username and password
		Contribute to sensitive data
		Prevent data leaks
		Restrict access rights based on RBAC
		VPN access rights restrictions for secure access
	Use of Virtual Private Networks (VPNs)	Utilizing VPNs for secure access
		Providing VPN access by IT teams
	Non-Disclosure Agreement (NDA)	Use of patient data
		Penalties for NDA violations

Encryption

Based on the research findings, implementing encryption for diagnostic data and patient information is a critical effort in maintaining the confidentiality of sensitive medical information, ensuring it is accessible only to authorized personnel. Encryption plays a vital role in protecting data against the risks of unauthorized access, information leakage, and potential data misuse. The research results indicate that RSUD Bakti Pajajaran has implemented a data security system utilizing the Advanced Encryption Standard (AES) algorithm, which is widely recognized for its high level of security and robust resistance to various cryptographic attacks. The application of this algorithm ensures data protection both during storage (data at rest) and throughout the information exchange process (data in transit), thereby preserving the confidentiality and security of electronic medical records.

This aligns with research by Ranaweera and Colombo (2024), which asserts that the rapid digitalization of medical records and the increasing reliance on electronic communication in healthcare necessitate robust security measures to protect sensitive patient data (Ranaweera & Colombo, 2024).

Confidentiality Access Control

Based on the analysis results, confidentiality access control is a crucial component of the information security system at RSUD Bakti Pajajaran through the use of the MediFirst application. Each user is granted access rights aligned with their duties and responsibilities, ensuring that the implementation of Role-Based Access Control (RBAC) effectively restricts information access and prevents data misuse. The authentication mechanism is implemented using individual usernames and passwords, supported by biometric authentication (fingerprint recognition) in certain parts of the system to bolster access security. Through the implementation of these access controls and authentication measures, the confidentiality of medical record information is well-maintained, thereby optimally supporting patient data protection.

This aligns with research by Wardani et al. (2024), which highlights that in terms of access control, patient data security is a top priority for healthcare systems, particularly concerning sensitive data such as Electronic Medical Records. Access control is key to ensuring this security. Effective access control ensures that sensitive health data can only be accessed by authorized personnel, thereby reducing the likelihood of unauthorized access. Secure access control is crucial in preventing data breaches by strictly regulating access to sensitive patient data (Wardani et al., 2024)

The Use of Virtual Private Networks (VPN)

Based on the analysis results, the use of Virtual Private Networks (VPN) demonstrates the organization's efforts to ensure that data exchange processes are conducted through secure communication channels protected by encryption. The granting of VPN access, managed by the Information Technology (IT) team, reflects strict access controls and restrictions, ensuring that only authorized users can access the system. The implementation of this mechanism plays a crucial role in

maintaining the security and confidentiality of medical record information, particularly when the system is accessed from outside the hospital's internal network.
This aligns with research by Wahyudi and Purnama (2019), which indicates that the implementation of a VPN allows data exchange to occur through secure and encrypted communication channels, thereby reducing the risk of data leakage during the transmission process (Wahyudi & Purnama, 2019).

Non- Disclosure Agreements (NDA)
Based on the analysis results, the use of patient data must be handled with utmost care and utilized solely for healthcare service purposes in accordance with authorized access. To prevent information misuse, healthcare facilities impose sanctions on individuals who violate the provisions of the Non-Disclosure Agreement (NDA), particularly in the event of unauthorized data leakage or disclosure. Furthermore, the implementation of digital signatures, which can only be executed by authorized personnel, serves as a crucial control measure to ensure that all access and approvals related to patient data are performed exclusively by individuals with the appropriate rights. The NDA functions as a binding legal foundation for healthcare professionals and related staff, preventing them from disseminating patient data outside the scope of healthcare services.
This aligns with research by Ariyanti (2024), which states that NDAs serve as a binding legal foundation for healthcare workers and hospital staff in maintaining the confidentiality of patient medical information. The study emphasizes that the inclusion of legal and administrative sanctions within NDAs can significantly improve staff compliance with data confidentiality principles.

Identifying the security of medical record data and information in terms of Integrity factors *(Integrity)*

Table 2 Implementation of Integrity *(Integrity)*

Theme	Category	Coding
Implementation of Integrity *(Integrity)*	Integrity Access Control	Account usage discrepancies
		Violations detected through audit logs
		Backups restored to ensure integrity
		Changes to data
	Use of Hash Functions	Hash Implementation
		Data Integrity with Hashes
		Detecting Hash and Value Differences
		The Importance of Hash Functions
	Digital signature	Digital signatures are only valid for authorized parties.
		Digital signature validity
		Data security-related uses
		Signatures do not yet use barcodes.
	Audit and Logging	Activity through records
		Transparent and accurate audit trail
		The RM Installation Head reviews the audit trail
		The audit trail records user activity
	Patch and Update Management	Evaluate the impact of updates before implementation
		Updates are tested through a pilot phase
		Patch delays can lead to vulnerabilities
		Testing is performed regularly

		Systems are updated regularly

Integrity Access Control

Based on research at Bakti Pajajaran Regional Hospital, data recovery is performed through backup and restore mechanisms to ensure the integrity of medical record information is maintained in the event of system disruptions, technical errors, or data loss. The restore process allows data to be returned to its last valid and verified state, thus maintaining the accuracy, integrity, and consistency of the information after the recovery process. While backups are generally related to availability, their implementation during the recovery phase plays a crucial role in maintaining data integrity by preventing unauthorized changes or damage. Furthermore, discrepancies in account usage indicate potential access breaches that could impact data integrity, necessitating stricter access rights controls according to user roles. The use of audit logs, which record all user activity, allows for the detection and tracking of any data changes, thus supporting the monitoring and evaluation process in the event of data integrity breaches.

This aligns with research by Prabwati Maia et al., 2025. In terms of security, integrity refers to efforts to ensure that medical data remains accurate, intact, unaltered without authorization, and trustworthy for both medical personnel and patients. Maintaining this integrity is crucial because invalid or manipulated data can have devastating consequences for medical decision-making. For example, implementing an audit log system in the EMR electronic medical record (Prabwati Maia et al., 2025) is a practical approach.

Using Hash Functions

Based on the analysis, the implementation of hash functions is used as a mechanism to maintain the integrity of medical record data by ensuring that stored information is not altered without authorization. Data integrity can be verified by comparing the hash values generated before and after the data storage or access process.

This is in line with research by (Sha- et al., 2024), which states that hashes are a fundamental component of cybersecurity architecture. Their primary function is to convert variable-length input data into a fixed-length output, known as a hash value (Sha- et al., 2024).

Digital Signatures

Based on the results at Bakti Pajajaran Regional Hospital, the use of digital signatures is limited to authorized personnel, ensuring that any approval or validation of medical record documents can be accounted for. The validity of digital signatures is crucial for ensuring the authenticity of the signatory's identity and ensuring that the document remains unchanged after it is signed.

This aligns with research by (Fitriyah et al., 2022). Every electronic system provider must operate the electronic system reliably and securely and is responsible for ensuring its proper operation. The use of digital signatures in electronic medical record transactions serves as a tool for authentication and verification of the signatory's identity and the integrity and authenticity of the electronic information (Fitriyah et al., 2022).

Audit and Logging

Based on the analysis, the electronic medical records system systematically uses an audit trail to ensure the recording process is transparent and accurate. The audit trail records every user activity, allowing all actions taken within the system to be traced.

This aligns with Minister of Health Regulation No. 24 of 2022 concerning Medical Records, which mandates that audit trails be a mandatory element in hospital information systems. Audit trails not only play a role in oversight but also serve as a crucial tool in identifying potential access abuse and privacy violations (Ministry of Health, 2022).

Patch and Update Management

Patch and Update Management ensures that all operating systems and applications are continuously

updated with the latest security patches to protect against vulnerabilities that could be exploited to compromise data (Agung Wijoyo et al., 2023).
Based on the analysis, each system update must be evaluated to assess its impact before full implementation, to ensure it does not disrupt service functionality and data security. The update process is conducted through a trial phase to identify potential errors or system disruptions early.

Identifying the security of medical record data and information in terms of availability factors *(Availability)*

Table 3 Availability Implementation *(Availability)*

Theme	Category	Coding
Availability implementation *(Availability)*	Redundancy and Failover	Data is stored on a separate server.
		Failover is performed automatically.
		Database and network duplication
		Placement outside the hospital's main server
		Implementation of redundancy and failover
		Backup system failure
	Data Backup	Data backup and disaster recovery
		Data backups are performed once a month
		Data backups are performed regularly
		Data backups are performed once a week
		Data backups are stored in the cloud
	Disaster Recovery	Manual data re-entering after system recovery
		Disaster recovery simulation within a year
		RM head coordinating and reviewing the recovery process
		Data recovery from backup
		Recovery against the recovery team objective
	Maintenance and Updates	Routine server checks
		Proposed system improvements
		Performed during low-activity times
		System is under maintenance and is active
	Performance Measurement and Monitoring	Responding to detected suspicious activity
		Server failures
		Minimizing downtime
		Using real-world simulations for interactivity
		Connection drops or slow downs due to network issues
		Continuous monitoring
		Violations detected through audit logs

Redundancy and *Failover*
Based on the analysis, the medical records information system utilizes redundancy and failover to

maintain service availability and data security. Medical record data is stored on a separate server located outside the hospital's main server, minimizing the risk of data loss in the event of a disruption to the main system.
This aligns with research by (We'e et al., 2023). To support these needs, a redundant network is essential. Redundancy minimizes downtime, meaning that if one network goes down, it will switch to a backup network (We'e et al., 2023).

Data Backup
Based on the analysis results, data backup processes are conducted on a routine basis, both weekly and monthly, to minimize the risk of data loss. The backups are stored via the cloud, ensuring that the reserve data remains secure and can be easily retrieved when needed.
This aligns with research by Widiyanti et al. (2024), which states that electronic medical record systems have implemented periodic data backups and stored reserve data on separate servers or in the cloud to maintain data availability in the event of system disruptions (Widiyanti et al., 2024).

Disaster Recovery
Based on the analysis results, medical record data that is recorded manually during system downtimes is re-entered into the information system once it resumes normal operation. The disaster recovery process is carried out periodically through simulations at least once a year to ensure the readiness and effectiveness of the data recovery procedures.
This aligns with research by Haryadi et al. (2019), which highlights that disaster recovery is a crucial component of information security management, aimed at minimizing the impact of data loss and service disruptions caused by unexpected events (Haryadi et al., 2019).

Maintenance and Updates
Based on the findings, the servers undergo routine inspections to ensure stable performance. Maintenance processes are generally scheduled during periods of low user activity to avoid disrupting hospital operations. During maintenance periods, the system is temporarily deactivated and subsequently reactivated once the inspection is complete.
This aligns with research by Setiawan (2025), which asserts that the routine maintenance of electronic medical record systems, coupled with data backups stored across various storage media, ensures that data remains available whenever needed (Setiawan, 2025).

Performance Measurement and Monitoring
Based on the analysis results, the system is equipped with continuous monitoring mechanisms to detect suspicious activities and potential breaches through audit logs. In the event of a server failure or network disruptions, such as slow or dropped connections, incident management is executed rapidly to minimize downtime. Furthermore, practical simulations are employed to test the system's response and enhance readiness in handling operational disruptions.
This aligns with research by Rusdiana et al. (2024), which states that monitoring the performance of electronic medical record systems—encompassing aspects of availability and data accuracy—is an integral part of health information system management. The evaluation of these indicators must be conducted periodically to ensure the quality, reliability, and continuity of health information services (Rusdiana et al., 2024).

Conclusion
Regarding the Confidentiality aspect, the MediFirst application utilizes individual authentication mechanisms in the form of usernames and passwords for each user. This ensures that access to medical record data is strictly restricted according to the respective authority of each staff member. Additionally, the system is capable of recording user login activities as a form of oversight and to support internal audit processes.
In terms of the Integrity aspect, the MediFirst application strives to maintain the accuracy and

completeness of medical record data through access right restrictions and user activity logging. This mechanism serves to minimize the risk of data alteration by unauthorized parties.
Concerning the availability aspect, the MediFirst system is considered to adequately support smooth service operations, as medical record data can be accessed by authorized personnel according to service needs. Ongoing system maintenance efforts and support from information technology staff contribute to maintaining system availability, although potential technical disruptions and network dependency remain challenges that require careful attention.

Conflict of Interest
The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Ethical Considerations
This research has undergone an ethical review process and has been granted ethical clearance in accordance with applicable research ethics guidelines and principles. Ethical approval was obtained from the Research Ethics Committee of Bakti Pajajaran Regional General Hospital (RSUD Bakti Pajajaran), which is the authorized body for conducting ethical assessments of research within the hospital environment. The ethical approval for this study is evidenced by the Ethical Clearance Certificate number: 000.9.2/2376-um.

Use of Artificial Intelligence (AI)
The authors have nothing to declare regarding the use of Artificial Intelligence (AI) in the generation of the research content. However, the authors state that AI was utilized solely to assist in translating this manuscript into English.

Conflict of Interest Statement
The authors declare no potential conflicts of interest concerning the research, authorship, and publication of this article.

Funding
The authors received no funding from any source for this study.

Acknowledgments
The author would like to express their gratitude to all parties at RSUD Bakti Pajajaran who granted permission and facilitated the smooth execution of the research procedures, as well as to all the medical record staff who willingly served as informants. The author is also deeply grateful to their academic advisor for consistently providing moral and material support, and to their friends for their continuous motivation and encouragement until the completion of this work.

Author Contributions
FSH collected the data, analyzed the data, wrote, and revised the manuscript. NAR provided research supervision, methodological guidance, and reviewed the manuscript. NAR, BAS, and LI provided critical feedback during the writing process.

References
Agung Wijoyo, Ade Rosadi, Fadhil Is Hakim, Muhamad Hanafi, & Sidik, R. (2023). Keamanan Jaringan Melindungi Sistem dari Serangan Luar. *Jurnal Riset Informatika Dan Inovasi*, *1*(3), 1–3.

Amin, M., Setyonugroho, W., & Hidayah, N. (2021). Implementasi Rekam Medik Elektronik: Sebuah Studi Kualitatif. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(1), 430–442. https://doi.org/10.35957/jatisi.v8i1.557

Annisa, O., & Tria, S. P. (2020). *Tinjauan Implementasi Sistem Informasi Manajemen Rumah Sakit (Simrs) Di Unit Rekam Medis Rsud Bangka Tengah*. *01*(03), 1–10.

Cholik, C. A. (2021). Teknologi Informasi, ICT,. *Jurnal Fakultas Teknik*, *2*(2), 39–46.

Fitriyah, Y., Riasetiawan, M., Lazuardi, L., Sanjaya, G., & Mada, G. (2022). *Analisis Tingkat Kesiapan Implementasi Tanda Tangan Digital Untuk Autentikasi Dokumen Rekam Medis Elektronik di Instalasi Rawat Jalan RSUD Kota Yogyakarta*. *7*(2), 52–69.

Haryadi, E., Abdussomad, & Robi. (2019). *Implementasi Sistem Backup Data Perusahaan Sebagai Bagian dari Disaster Recovery Plan*. *29*(2), 6–11.

Herisasono, A. (2024). *Perlindungan Hukum terhadap Privasi Data Pasien dalam Sistem Rekam Medis Elektronik Legal Protection of Patient Data Privacy in Electronic Medical Record Systems*. *7*(12), 4677–4681. https://doi.org/10.56338/jks.v7i12.6620

Kemenkes, R. (2022). Peraturan Menteri Kesehatan RI No 24 tahun 2022 tentang Rekam Medis. *Kemenkes Republik Indonesia*, *151*(2), 1–19.

Kemenkes, R. (2023). *Undang-Undang Republik Indonesia tentang Kesehatan Pasal 1 ayat 1*. *187315*, 1–300.

Listyorini, I. puguh, & Sintya, I. (2021). Sistem Keamanan SIMRS di Rumah Sakit. *Prosiding Seminar Informasi Kesehatan Nasional (SIKesNas)*, 234–240.

Prabwati Maia, D. L., Ikawati, R. F., & Afifah, L. (2025). *Tinjauan Keamanan Data Rekam Medis Elektronik Di Puskesmas Jabung Review of Electronic Medical Record Data Security at Puskesmas Jabung*. 87–94.

Rabia, D. P., & Dety Mulyanti. (2023). Tantangan SIMRS dalam Penerapan Rekam Medis Elektronik Berdasarkan Permenkes 24 Tahun 2022: Literature Review. *Jurnal Medika Nusantara*, *1*(1), 18–28. https://doi.org/10.59680/medika.v1i1.288

Ranaweera, A., & Colombo, C. (2024). *Komunikasi Data Medis yang Aman: Pendekatan Komprehensif dengan Enkripsi AES. February*. https://www.researchgate.net/publication/378261261

Rusdiana, A., Yogaswara, D., & Annashr, N. N. (2024). *ANALISIS IMPLEMENTASI REKAM MEDIS ELEKTRONIK BERDASARKAN FAKTOR HOT-FIT DI PUSKESMAS KAWALU KOTA*. *20*(2), 108–126.

Setiawan, R. (2025). *Integrasi Teknologi Blockchain untuk Kontrol Akses yang Aman dalam Basis Data Terdistribusi*. *3*(2), 379–384.

Sha-, A., Sitorus, N., Sharon, J., Sinaga, G., & Samosir, S. L. (2024). *Analisis Kinerja Algoritma Hash pada Keamanan Data : Perbandingan*. *2*(2).

Sugandi, M. A., & Halim, R. M. N. (2020). Analisis End-User Computing Satisfaction (Eucs) Pada Aplikasi Mobile Universitas BiSugandi, M. A., & Halim, R. M. N. (2020). Analisis End-User Computing Satisfaction (Eucs) Pada Aplikasi Mobile Universitas Bina Darma. Sistemasi, 9(1), 143. https://doi.org. *Sistemasi*, *9*(1), 143.

Wahyudi, M., & Purnama, R. A. (2019). *Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP (Performance Analysis Site to Site IP Security Virtual Private Network (VPN) with Algorithm Encryption ISAKMP)*. *7*(November), 129–135.

Wardani, E., Putra, H. D., Sonia, D., & Yulia, N. (2024). *Keamanan Sistem Informasi Rekam Medis Elektronik di Rumah Sakit Islam Jakarta Sukapura*. *3*(2), 31–38.

We'e, A., Nugroho, H., & Siswatibudi, H. (2023). Evaluasi Aspek Keamanan Dan Kerahasiaan Rekam Medis Elektronik Di Rumah Sakit Panti Nugroho. *Jurnal Permata Indonesia*, *14*(2), 72–81. https://doi.org/10.59737/jpi.v14i2.265

Widiyanti, W. S., Hastuti, M. N., & Kusumawati, A. E. (2024). *Indonesian Journal of Health Information Management (IJHIM) Vol . 4 No . 2 (2024), 1 Tinjauan Keamanan Data Rekam Medis Elektronik P a d a A p l i k a s i S i m p u s B e r d a s a r k a n A s p e k Confidentiality , Integrity , Dan Availability Di Pu*. *4*(2), 1–6.