Indonesian Journal of Global Health Research
Volume 8 Number 2, April 2026
e-ISSN 2715-1972; p-ISSN 2714-9749
http://jurnal.globalhealthsciencegroup.com/index.php/IJGHR

EVALUATION OF ELECTRONIC MEDICAL RECORD QUALITY FROM THE PERSPECTIVE OF DATA SECURITY

Riska Rosita*, Yunita Wisda Tumarta Arif, Naufal Rohman Wachid
Universitas Duta Bangsa Surakarta, Jl. K.H Samanhudi No.93, Sondakan, Laweyan, Surakarta, Jawa Tengah 57147, Indonesia
*riska_rosita@udb.ac.id

ABSTRACT
All health care facilities in Indonesia are required to implement Electronic Medical Records (EMR), including Community Health Centers. The implementation of EMR has various challenges such as the threat of electronic data theft, data loss, and data leakage Objective: to evaluate the quality of EMR data security at Community Health Center X based on the Peraturan Menteri Kesehatan nomor 24 tahun 2022. This is a descriptive qualitative study with a cross-sectional approach. The subjects of the study were 8 respondents, namely, including registration unit officers, general practitioner, midwife at a maternal and child health (KIA) clinic, laboratory head, administrative head, pharmacy staff member, and medical records head. The object of the study is the EMR system. Data collection through observation checklists and in-depth interviews. Observation data were analyzed descriptively, while interview data were analyzed with thematic/framework analysis. The study shows that based on the confidentiality aspect, all officers still use the same account when logging into EMR. Community Health Center X does not yet have a feature to document the audit trail process. In terms of integrity, the use of digital signatures is replaced with clear names filled in using passwords. In terms of availability, Community Health Center X stores patient data on the server and has backed up data periodically, EMR has an ID feature to download patient data. Data security is important in the implementation of the Electronic Medical Records (EMR) system to ensure the quality and confidentiality of medical information.

Keywords: availability; confidentiality; integrity; medical data; RME

How to cite (in APA style)
Rosita, R., Arif, Y. W. T., & Wachid, N. R. (2026). Evaluation of Electronic Medical Record Quality from the Perspective of Data Security. Indonesian Journal of Global Health Research, 8(2), 147–154. https://doi.org/10.37287/ijghr.v8i2.795.

INTRODUCTION

All healthcare facilities in Indonesia are required to implement Electronic Medical Records (EMR). This mandate applies to primary healthcare facilities including clinics, community health centers (Puskesmas), and general practitioners secondary facilities that involve specialist physicians, and tertiary or referral facilities that involve subspecialist physicians. The integration of EMR across these levels is intended to ensure that patients' medical data remain connected and accessible as they move from primary to tertiary care (Rudiantoro, Suprapto and Agustin, 2025) (Agus, Ratnaningsih and Santoso, 2019). However, the implementation of EMR still faces various ethical and legal challenges. Among the major concerns are issues related to privacy breaches, data security, data ownership, and legal accountability (Kundari, Aji and Rejeki, 2025)(Agustin et al., 2020).

Electronic Medical Records (EMRs) contain patients' personal information that is stored electronically and associated with their diagnosis and treatment; therefore, the confidentiality and security of medical data must be strictly protected (Yang et al., 2020) (Kaplan, 2020). According to the Ministry of Health Regulation (Kemenkes, 2022), the implementation of Electronic Medical Records must ensure compliance with essential data and information security principles, namely confidentiality, integrity, and availability. Survey data from the Surakarta City Health Office revealed that one of the community health centers (Puskesmas X) in Surakarta has developed its own electronic medical record (EMR) system as an innovation to support digital-based patient care services. However, since the system is still in the developmental stage, it remains vulnerable to

various issues that may compromise data security. Internal security threats include the potential misuse of patients' medical data by staff members who share the same user account and password interchangeably. Meanwhile, external threats involve cyberattacks such as hacking, malware, and ransomware, which can lead to data theft, loss, or manipulation (Usman and Qamar, 2020). The theft of patient data can result in both material and psychological harm to victims, particularly when their identity and health information are exposed and used to discriminate against them (Półchłopek et al., 2020). Such incidents of personal data misuse indicate systemic weaknesses or insufficient supervision, potentially causing significant harm to data owners (Situmeang, 2021).

Based on these issues, this study aims to evaluate the quality of data security in the Electronic Medical Records (EMR) system of Community Health Center X against the requirements of Regulation of the Minister of Health of the Republic of Indonesia No. 24 of 2022 (Medical Records) by assessing compliance across key controls confidentiality, integrity, and availability (including access authorization and authentication), user account management, audit trails, digital signatures/verification, data backup, and disaster recovery). This effort aims to strengthen data protection practices and improve the overall reliability of EMR management in primary care settings in Indonesia.

METHOD

This study employed a descriptive qualitative design using a cross-sectional approach. The research was conducted at Community Health Center (Puskesmas) X, located in Surakarta City, Indonesia. Data were collected through direct observation, in-depth interviews, and literature review conducted at the study site. The informants consisted of eight respondents involved in electronic medical record management, including registration unit officers, general practitioner, midwife at a maternal and child health (KIA) clinic, laboratory head, administrative head, pharmacy staff member, and medical records head. The object of the study was the Electronic Medical Record (EMR) system implemented at the Community Health Center. Data were collected through observations and interviews. The evaluation was guided by the Confidentiality–Integrity–Availability (CIA) framework aligned with national requirements (PMK No. 24/2022), with operational indicators defined a priori for access control and accountability (confidentiality), accuracy, correction governance and verification (integrity), and real-time access, reporting/export, and backup/disaster recovery (availability). These variables represent the core dimensions of information security, which together determine the reliability and protection level of electronic medical record systems in healthcare facilities.

RESULT

EMR Data Security Based on Confidentiality Aspect

According to the Ministry of Health Regulation (PMK) No. 24 of 2022 concerning Medical Records, emphasizes that the confidentiality of medical records serves as a guarantee of data and information security against both internal and external threats from unauthorized parties. This principle ensures that the data and information contained in electronic medical records are protected from misuse and unauthorized dissemination. The evaluation of EMR data security quality in terms of confidentiality was assessed through several indicators. The first indicator is identification, which refers to the process by which EMR users are required to provide specific credentials, such as usernames, identification numbers, or biometric data to access the system (Pradita, Kusumo and Rahmawati, 2022).

At Puskesmas X, this principle has been implemented through a Standard Operating Procedure (SOP) numbered KS.00/1915/IX/2022, which regulates access rights to the EMR system. Access is granted only to authorized healthcare personnel who have formally sworn to maintain the confidentiality of patient medical information. These personnel include staff members from the registration unit, general polyclinic, emergency department, dental and oral clinic, maternal and

child health (MCH) clinic, family planning services, immunization unit, acupuncture clinic, counseling services, pharmacy, and laboratory. Furthermore, the SOP for EMR implementation established by healthcare facility leadership is required to define clear access control policies to ensure that only eligible personnel can retrieve or manage electronic medical records. This policy aligns with the provisions of PMK No. 24 of 2022, which mandates that access rights to EMRs must be explicitly defined within the institution's operational procedures.

The second indicator is authentication, which refers to the system's process of verifying the identity of users who have been previously identified. An Electronic Medical Record (EMR) system should be capable of authenticating users through various security mechanisms, such as passwords, personal identification numbers (PINs), tokens, smart cards, or biometric identifiers including fingerprints or facial recognition. The third indicator is authorization, which refers to the process of granting access rights to users based on their roles and responsibilities within the healthcare organization. Authorization defines the scope of data and functions that users are permitted to access after they have been properly identified and authenticated. A well-designed authorization system safeguards the confidentiality and security of electronic medical record (EMR) data by ensuring that only authorized personnel such as physicians, nurses, and administrative staff can access information relevant to their duties (Mardiana and Arsanti, 2023). At Puskesmas X, no formal written policy has yet been established to regulate user authorization based on roles and authority. The existing policy only covers the Standard Operating Procedure (SOP) for entering patient medical record data. Therefore, it is strongly recommended that the healthcare facility develop a specific regulation or SOP addressing user authorization in EMR systems. Such a policy is essential to strengthen data access control and align institutional practices with national standards for medical record data security.

The fourth indicator is accounting (accountability), which refers to maintaining a comprehensive log of all activities related to access and use of electronic medical record (EMR) data. Ideally, this function records who accessed the data, when the access occurred, and what changes were made to the records. However, the information system implemented at Puskesmas X has not yet been equipped with such accountability features. Currently, all users of the SIMPUS application can edit or delete medical data without traceability or user identification (Rahman, 2024). This condition poses a significant risk to data security, as the absence of an accountability mechanism prevents the detection of unauthorized activities or misuse.

EMR Data Security Based on Integrity Aspects

According to the Ministry of Health Regulation (PMK) No. 24 of 2022 concerning Medical Records, stipulates that integrity serves as a guarantee of the accuracy of data and information contained in the Electronic Medical Record (EMR), and that any modification to the data may only be performed by individuals who are granted authorized access rights. The second indicator is data correction management, which refers to the existence of clear policies and procedures governing how data corrections are made within the Electronic Medical Record (EMR) system. At Puskesmas X, medical record data are stored in accordance with the original information entered, following proper and consistent mechanisms. However, the facility has not yet established a clear policy that specifies who is authorized to perform data corrections and how such corrections should be executed.

Furthermore, the current information system at Puskesmas X lacks the capability to record every data modification in an activity log, which would enable traceability and accountability over time. This practice is not yet aligned with the provisions of the Ministry of Health Regulation (PMK) No. 24 of 2022, which stipulates that data corrections may only be performed by authorized healthcare providers and administrative staff including medical record officers within a maximum period of 2x24 hours after data entry.

EMR Data Security Based on Availability Aspect

According to the Ministry of Health Regulation (PMK) No. 24 of 2022 concerning Medical Records, stipulates that availability ensures that the data and information contained in the Electronic Medical Record (EMR) can be accessed and utilized by authorized individuals as determined by the leadership of the healthcare facility. The availability of EMR data encompasses two main aspects. The first is data availability for patient care, which aims to support the processes of diagnosis, treatment, and patient management. Therefore, patient data must be readily available in real time and easily accessible to healthcare professionals who are directly responsible for patient care, enabling them to provide accurate and timely medical services (Rosita, Risqika, *et al.*, 2024)(Lee *et al.*, 2025).

Such data include essential medical information such as patient medical history, examination results, prescriptions, physicians' notes, and other relevant records that serve as the basis for clinical decision-making (Rosita, Wisda, *et al.*, 2024). Given that medical data are highly personal and sensitive, access to this information must be strictly regulated and limited only to authorized personnel who are directly involved in patient care. Ensuring appropriate access control is therefore crucial to maintain both data security and service quality within healthcare facilities.

The second aspect of data availability focuses on administrative and managerial needs. In addition to supporting clinical care, EMR data are also required for reporting to authorized agencies or regulatory bodies and for analyzing the performance of healthcare facilities. Such data include statistical information related to the number of patients, types of services provided, disease incidence, performance outcomes, and other operational aspects used for financial reporting, auditing, and strategic planning (Puspitarini, Bukhori and Nuryadi, 2025).

For reporting purposes, the data are generally processed and presented in formats that remove patient identifiers to protect individual privacy in accordance with applicable regulations (Sofia *et al.*, 2022). Access to these datasets is restricted to administrative staff, managers, and authorized personnel responsible for evaluation, planning, and decision-making at the management level. At Puskesmas X, the Electronic Medical Record (EMR) system has been equipped with a data export feature to ensure the availability and accessibility of patient data when needed. This feature allows patient data to be retrieved at any time for reporting purposes, thereby supporting policy formulation and administrative decision-making within the healthcare facility. Strengthening this functionality contributes to enhancing data transparency, improving institutional accountability, and ensuring that information remains available for continuous quality improvement and compliance monitoring.

DISCUSSION

The results of this study emphasize that the quality of Electronic Medical Records (EMRs) from the perspective of data security is determined by the interrelated principles of confidentiality, integrity, and availability. These three dimensions form the foundation of the data security framework known as the CIA Triad, which collectively ensures that medical information is protected, accurate, and accessible only to authorized users. The findings at Puskesmas X reveal that although efforts to implement digital record systems have been initiated, there were still several gaps in achieving optimal data protection practices in accordance with the Minister of Health Regulation (PMK) No. 24 of 2022 concerning Medical Records.

Confidentiality represents the ethical and legal cornerstone of patient data protection. At Puskesmas X, the use of user identification and authentication demonstrates a basic understanding of safeguarding sensitive information. However, the absence of formal written policies on authorization and accountability weakens the overall security posture. Without a well-defined access control system and audit trail, patient data remain vulnerable to internal misuse and external

breaches. This is consistent with earlier studies (Oh et al., 2021)(Ganiga et al., 2020) showing that incomplete implementation of confidentiality protocols can erode patient trust and institutional credibility in digital health services. Strengthening authentication systems, ensuring role-based access rights, and performing routine security audits are thus essential steps to reinforce data confidentiality and align practice with national standards. Strong authentication is critical to prevent data breaches and unauthorized access to EMR systems (Rosita, Risqika, et al., 2024). Users of EMR systems are also responsible for maintaining the confidentiality and security of patient data to prevent both misuse and data leakage (Yudianti and Arini, 2024). Compromised medical data can be exploited by irresponsible parties to commit cybercrimes, potentially resulting in material losses and psychological harm to affected individuals (Zahra, Hapsari and Safitri, 2024). Therefore, strengthening authentication mechanisms and user awareness is essential to ensure the quality and integrity of EMR data security.

An effective EMR system should maintain detailed audit trails documenting every access and modification to medical data. These records are essential to ensure transparency, enable systematic audits, and detect as well as prevent potential violations of access rights or data manipulation (Wijayanto, 2008). Strengthening the accountability function within EMR systems is therefore critical to improving overall data integrity and reinforcing patient trust in digital health record management. Integrity, on the other hand, serves as an indicator of data reliability and accuracy within the EMR system. While Puskesmas X has applied consistent data entry procedures, the lack of explicit policies regarding data correction and tracking mechanisms indicates limited assurance of data veracity. The inability of the system to record all data changes in a traceable log could potentially lead to discrepancies that compromise clinical and managerial decision-making. The literature underscores that maintaining data integrity is crucial to preventing diagnostic errors, delays, and miscommunication among healthcare teams. Implementing verification tools, time-bound correction procedures, and systematic standard operating procedures will help maintain data credibility and ensure that the EMR functions as a trustworthy source of clinical evidence.

The evaluation of EMR data security quality from the perspective of integrity includes the assessment of data accuracy, ensuring that the information stored in the EMR system corresponds precisely to the original data entered (Schmidt et al., 2019). All EMR users at Puskesmas X are required to input data correctly and consistently in accordance with standardized procedures (Melnick et al., 2020) (Tekayana et al., 2024). Data verification prior to storage is crucial to prevent errors and inconsistencies. Moreover, the establishment of clear Standard Operating Procedures (SOPs) that define systematic data management practices is essential to maintain data accuracy and reliability. These measures are vital to ensure that medical information remains dependable for both clinical decision-making and healthcare management processes, thereby supporting the overall quality and safety of health services (Sinaga and Sumartini, 2019).

Ministry of Health Regulation (PMK) No. 24 of 2022 stipulates that data corrections can only be made by health service providers and administrative staff, including authorized medical records officers, within a maximum period of 2x24 hours from data entry. This regulation underscores the importance of timely and accurate data correction to maintain the reliability and accuracy of patient medical information (Yuliani, Noor and Maryati, 2024). Failure to comply with this provision can lead to delays in disease diagnosis and reduce the accuracy of medical data (Maulindar, Guterres and Rosita, 2023). Both factors may compromise patient safety and diminish the overall quality of healthcare services provided by health facilities (Sari, Mediawati and Yudianto, 2019).

Availability complements the previous two dimensions by ensuring that data are accessible whenever needed while maintaining security control. In Puskesmas X, the establishment of real-time access and daily data backups indicates progress in supporting service continuity and resilience against potential data loss. These measures are vital in mitigating the impact of system failures,

natural disasters, or cyber incidents. The ability to recover data efficiently ensures that patient care processes remain uninterrupted, thereby enhancing both operational stability and patient satisfaction. In addition, proper management of data availability for administrative and reporting purposes allows healthcare facilities to perform evidence-based planning, evaluation, and compliance monitoring without compromising patient privacy.

Puskesmas X has also implemented several preventive measures to mitigate the risk of data loss by creating patient data backups stored on a secondary server. The data backup process is performed daily by the IT staff to ensure that all medical records are securely replicated. In the event of data loss caused by natural disasters, system failures, or cyber incidents such as data theft, Puskesmas X can promptly restore patient data from the backup server. This initiative aligns with the provisions of the Ministry of Health (Kemenkes, 2022), which emphasize that the establishment of a backup system plays a crucial role in maintaining the continuity of healthcare services. A well-managed data backup system enables healthcare facilities to recover information efficiently, thereby minimizing service disruptions and ensuring that patient care activities remain uninterrupted. Moreover, the ability to restore data swiftly contributes not only to operational resilience but also to patient satisfaction and perceived service quality (Agus, Ratnaningsih and Santoso, 2019).

Overall, the interplay between confidentiality, integrity, and availability illustrates that data security is not merely a technical concern but an integral component of healthcare quality management. The CIA triad provides a coherent lens for evaluating EMR quality: confidentiality builds trust through disciplined access control and auditable accountability (Cobrado et al., 2024)(Vankayala, 2025); integrity assures reliable information through governed correction, verification, and traceability (Wijayanti, Ujianto and Rianto, 2024); availability guarantees timely, secure access and rapid recovery when incidents occur (Mohebi et al., 2025). The literature converges on a practical roadmap that resonates with our context: mature role-/attribute-based access control and continuous audit (confidentiality), explicit and time-bound correction workflows with immutable logs (integrity), and routinely validated backup-and-recovery capabilities (availability). Aligning local SOPs with these elements can advance compliance, strengthen clinical reliability, and sustain service continuity in Indonesia’s primary-care EMR implementations.

CONCLUSION

This study shows that the quality of Electronic Medical Records (EMR) from a data security perspective depends on the implementation of three key aspects, as outlined in Minister of Health Regulation No. 24 of 2022: confidentiality, integrity, and availability. At Community Health Center X, basic controls such as authentication and routine backups have been implemented, but gaps remain in role-based authorization, audit trails, data correction management, and accountability. To improve the quality of EMR, healthcare facilities must strengthen governance by developing clear standard operating procedures, implementing secure authorization and audit systems, and ensuring regular data backups. Integrating these three aspects within an integrated information security framework will help maintain data reliability, protect patient privacy, and improve the overall quality of healthcare services.

ACKNOWLEDGEMENTS

The author would like to thank the " *Kementerian Pendidikan, Kebudayaan, Riset, Dan Teknologi Direktorat Jenderal Pendidikan Vokasi*" for the 2024 budget year for providing financial support for this research with contract number 022/UDB.LPPM/A.34-HK/III/2024.

REFERENCES

Agus, Ratnaningsih, T. and Santoso, W. (2019) ‘The Relationship Of Emr (Electronic Medical Record) Documentation Performance With Patient Satisfaction’, Indonesian Journal of Global Health Research, 7(1), pp. 63–68. Available at: https://doi.org/10.37287/ijghr.v2i4.250.

Agustin, R. et al. (2020) 'Tinjauan Etik Pembukaan Rahasia Medis dan Identitas Pasien pada Situasi Wabah Pandemi COVID-19 dan Kaitannya dengan Upaya Melawan Stigma Pasien Positif', Jurnal Etika Kedokteran Indonesia, 4(2), p. 41. Available at: https://doi.org/10.26880/jeki.v4i2.46.

Cobrado, U.N. et al. (2024) 'Access control solutions in electronic health record systems: A systematic review', Informatics in Medicine Unlocked, 49(May), p. 101552. Available at: https://doi.org/10.1016/j.imu.2024.101552.

Ganiga, R. et al. (2020) 'Security framework for cloud based Electronic Health Record (EHR) system', International Journal of Electrical and Computer Engineering, 10(1), pp. 455–466. Available at: https://doi.org/10.11591/ijece.v10i1.pp455-466.

Kaplan, B. (2020) 'Revisiting Health Information Technology Ethical, Legal, and Social Issues and Evaluation: Telehealth/Telemedicine and Covid-19', International Journal of Medical Informatics, 143(June), p. 104239. Available at: https://doi.org/10.1016/j.ijmedinf.2020.104239.

Kemenkes (2022) PMK No 24 Tahun 2022 Tentang Rekam Medis, Republik Indonesia.

Kundari, A., Aji, B. and Rejeki, D.S.S. (2025) 'Evaluation of the Implementation Of An Inpatient Electronic Medical Record System Using The Delone And Mclean Method', Indonesian Journal of Global Health Research, 7(5), pp. 1137–1142.

Lee, M. et al. (2025) 'Advancements in Electronic Medical Records for Clinical Trials: Enhancing Data Management and Research Efficiency', Cancers, 17(9), pp. 1–20. Available at: https://doi.org/10.3390/cancers17091552.

Mardiana, N. and Arsanti, M. (2023) 'Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia', Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia, 5(1), pp. 16–23. Available at: https://doi.org/10.52005/rechten.v5i1.108.

Maulindar, J., Guterres, J.X. and Rosita, R. (2023) 'Prediction and Prevention of Disease Diagnosis Delay Using Data Mining Methods in Healthcare Quality Management', Proceeding of International Conference on Science, Health, And Technology, pp. 80–86. Available at: https://doi.org/10.47701/icohetech.v4i1.3376.

Melnick, E.R. et al. (2020) 'The Association Between Perceived Electronic Health Record Usability and Professional Burnout Among US Physicians', Mayo Clinic Proceedings, 95(3), pp. 476–487. Available at: https://doi.org/10.1016/j.mayocp.2019.09.024.

Mohebi, S. et al. (2025) 'The impact of electronic medical records on clinical documentation: A case study', Journal of Education and Health Promotion, 14(June), pp. 1–6. Available at: https://doi.org/10.4103/jehp.jehp.

Oh, S.R. et al. (2021) 'A comprehensive survey on security and privacy for electronic health data', International Journal of Environmental Research and Public Health, 18(18). Available at: https://doi.org/10.3390/ijerph18189668.

Półchłopek, O. et al. (2020) 'Quantitative and temporal approach to utilising electronic medical records from general practices in mental health prediction', Computers in Biology and Medicine, 125(August), pp. 1–15. Available at: https://doi.org/10.1016/j.compbiomed.2020.103973.

Pradita, R., Kusumo, R. and Rahmawati (2022) 'Pentingnya Aspek Keamanan Informasi Data Pasien Pada Penerapan Rme Di Puskesmas', Journal of Sustainable Community Service, 2(2), pp. 52–62. Available at: https://transpublika.co.id/ojs/index.php/JSCS/article/view/437/366.

Puspitarini, N.W., Bukhori, S. and Nuryadi (2025) 'Evaluation Of Telemedicine Services In Outpatient Services At Hospital X, Jember District Using The Human Organization Technology Method (HOT-FIT MODEL)', Indonesian Journal of Global Health Research, 7(5), pp. 339–348.

Rahman, F.F. (2024) 'User Expectations And The Willingness To Adopt Electronic Medical Records In Primary Healthcare Ferry', Indonesian Journal of Global Health Research, 6(4), pp. 2317–2324. Available at: https://doi.org/10.37287/ijghr.v2i4.250.

Rosita, R., Risqika, A.M., et al. (2024) 'Evaluation of the Implementation of Outpatient Electronic Medical Records', in ISMoHIM, pp. 184–188.

Rosita, R., Wisda, Y., et al. (2024) 'Quality Evaluation on The Implementation of Electronic Medical Records in Primary Health Centers', in ICOHETECH, pp. 175–181.

Rudiantoro, D., Suprapto, I. and Agustin, S. (2025) 'The Implementation Of Electronic Medical Records On Performance Through Nurses' Workload And Completeness Of Nursing Care Documentation Danar', Indonesian Journal of Global Health Research, 7(3), pp. 335–342.

Sari, N., Mediawati, A.S. and Yudianto, K. (2019) 'Use Of The Technology Acceptance Model For Electronic Medical Records In Nursing Documentation: Scooping Review', Indonesian Journal of Global Health Research, 6(4), pp. 1953–1962. Available at: https://doi.org/10.37287/ijghr.v2i4.250.

Schmidt, M. et al. (2019) 'The Danish health care system and epidemiological research: From health care contacts to database records', Clinical Epidemiology, 11, pp. 563–591. Available at: https://doi.org/10.2147/CLEP.S179083.

Sinaga, N.C. and Sumartini, B. (2019) 'Effectiveness Of Electronic Medical Records On Patient Safety', Indonesian Journal of Global Health Research, 7(1), pp. 1095–1104. Available at: https://doi.org/10.37287/ijghr.v2i4.250.

Situmeang, S.M.T. (2021) 'Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber', Sasi, 27(1), p. 38. Available at: https://doi.org/10.47268/sasi.v27i1.394.

Sofia, S. et al. (2022) 'Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan', Jurnal Rekam Medik & Manajemen Informasi Kesehatan, 1(2), pp. 94–103. Available at: https://doi.org/10.47134/rmik.v1i2.29.

Tekayana, I.W.P. et al. (2024) 'Analysis of Factors Associated with the Use of an Electronic Medical Record Information System Based on the Technology Acceptance Model (TAM)', Indonesian Journal of Global Health Research, 6(4), pp. 2041–2048. Available at: https://doi.org/10.37287/ijghr.v6i4.3332.

Usman, M. and Qamar, U. (2020) 'Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology', Procedia Computer Science, 174, pp. 321–327. Available at: https://doi.org/10.1016/j.procs.2020.06.093.

Vankayala, V.N.M.K. (2025) 'Leveraging Identity and Access Management to Enhance Compliance Audits and Reduce Costs in Healthcare Environments', Sarcouncil Journal of Engineering and Computer Sciences, 4(8), pp. 91–96.

Wijayanti, D., Ujianto, E.I.H. and Rianto, R. (2024) 'Uncovering Security Vulnerabilities in Electronic Medical Record Systems: A Comprehensive Review of Threats and Recommendations for Enhancement', Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, 10(1), p. 73. Available at: https://doi.org/10.26555/jiteki.v10i1.28192.

Wijayanto, W. (2008) 'Bukti Audit Dalam Lingkungan Electronic Data Interchange (Edi)', Wahana: Jurnal Ekonomi, Manajemen dan Akuntansi, 11((2)), pp. 151–161.

Yang, M. et al. (2020) 'Teenager Health Oriented Data Security and Privacy Protection Research for Smart Wearable Device', Procedia Computer Science, 174(2019), pp. 333–339. Available at: https://doi.org/10.1016/j.procs.2020.06.095.

Yudianti, E.- and Arini, M.- (2024) 'Applying of Healthcare Failure Mode and Effect Analysis on Electronic Medical Record Implementation', Jurnal Kesehatan Vokasional, 9(1), p. 59. Available at: https://doi.org/10.22146/jkesvo.88541.

Yuliani, N., Noor, H.L. and Maryati, W. (2024) 'Quality of Medical Record Documentation Affects Accuracy of Diagnosis Codes In Ina-Cbgs Claims In Hospitals', Indonesian Journal of Global Health Research, 6(5), pp. 3237–3242. Available at: https://doi.org/10.37287/ijghr.v2i4.250.

Zahra, N., Hapsari, R.A. and Safitri, M. (2024) 'Legal Protection of Digital Identity Technology Through Identity Verification System Biometric-Based', Supremasi: Jurnal Pemikiran dan Penelitian Ilmu-ilmu Sosial, Hukum, & Pengajarannya p-ISSN, 19(1), pp. 86–98.