Global Economics and Finance Insights, Vol. 01, No. 01, PP 30-39, Year 2026

LITERATURE REVIEW: AUDIT OF MANAGEMENT INFORMATION SYSTEMS IN HOSPITALS TO IMPROVE PATIENT DATA SECURITY AND INTEGRITY

Seto Wahyu Prasetyo[1]

[1]Program Magister, Sekolah Tinggi Ilmu Ekonomi Indonesia Surabaya, Surabaya 60118, Jawa Timur, Indonesia
[*]setowahyuprasetyo@gmail.com

ABSTRACT

The development of Hospital Management Information Systems (SIMRS) and Electronic Medical Records (RME) improves the efficiency of healthcare services, but also poses risks to the security, confidentiality, and integrity of patient data. Sensitive medical data is vulnerable to leakage, manipulation, and unauthorized access if not supported by adequate controls. Therefore, information systems audits are an important instrument for evaluating the effectiveness of security controls and regulatory compliance. This study uses a qualitative approach with a systematic literature review method on publications in 2016–2026 from indexed national and international journals. The analysis is carried out through content analysis and thematic synthesis to identify security threats, audit frameworks, and improvement recommendations. The results of the study show that the threat is multidimensional, including technical, managerial, legal, and human aspects. Frameworks such as COBIT, ISO/IEC/IEEE standards, and the CIA Triad are effective in identifying security gaps. Innovations such as blockchain have the potential to strengthen trail audits and access controls. Standardized and continuous audits are key to improving security and maintaining public trust in digital healthcare.

Keywords: System Audit, Data Security, Literature Review, Hospitals

INTRODUCTION

The development of information technology has brought a major transformation to the health sector, especially in the management of patient data through various applications of Hospital Management Information System (SIMRS) and Electronic Medical Records (RME). With the increasingly centralized and integrated digital services in hospitals, the volume and sensitivity of patient data has increased significantly because it includes medical information, personal identity, diagnosis results, and patient medical history that is highly confidential. This also poses a high risk related to leakage, manipulation, or unauthorized access to patient medical data (privacy & security) if security controls are not properly managed (Asih et al., 2024).

Information systems audits are emerging as an important instrument for assessing the security, confidentiality, integrity and availability of patient data in SIMRS and RME. This audit process not only evaluates whether security mechanisms have been met according to applicable standards, but also identifies vulnerabilities that could threaten the quality of service and patient trust in the digital health system. Previous research has shown that framework-based audits such as COBIT 5/2019 are able to measure the level of security capabilities of hospital systems, as well as recommend necessary strategic improvements (Krisdiyawan and Kuswantoro, 2017).

The effective implementation of audits in SIMRS can provide an objective picture of the level of security risk and the readiness of the system in maintaining the confidentiality and integrity of patient data. Research by Setiatin & Azmi (2025) shows that although some hospitals have

implemented basic controls such as account management and individual access, there are weaknesses in technical security such as the lack of automatic logout features and password renewal policies, which have the potential to degrade the security quality of patient data.

In addition, other health information systems security studies emphasize that threat analysis, access control, data encryption, and regular risk evaluation are essential elements for maintaining the integrity and availability of medical information that is constantly evolving digitally. This shows that information system audits are not just administrative inspections, but also a comprehensive strategy to ensure that SIMRS runs safely and in line with high information security standards (Ahmad and Yusmanidar, 2025).

Therefore, research that focuses on auditing information systems in hospitals is essential to measure the extent to which the system can maintain the security, confidentiality, and integrity of patient data, as well as for the preparation of recommendations for improving policies, procedures, and technologies used. Each hospital needs to conduct systematic audits as part of its risk management and IT governance strategy to ensure patient trust and support the quality of health services effectively and responsibly.

THEORETICAL STUDIES

Management Information System

A Management Information System (SIM) is a system, which is an organized series of a number of parts/components that jointly function or move to produce information for use in company management (Alhadi, 2022). The definition of an information system is the relationship between four main parts which includes software, hardware, infrastructure, and trained human resources (Mardiah et al., 2018). The four main parts are interconnected to create a system that can process data into useful information. An information system is a collection of hardware and software designed to transform data into useful forms of information (Alandari, 2013). An information system is a system within an organization that brings together the needs of daily transaction management, supports operations, is managerial in nature and provides certain external parties with the required reports (Munthe et al., 2019). The Management Information System (SIM) is a system that processes and organizes data and information that is useful to support the implementation of tasks in an organization (Alhadi, 2022). Based on this understanding, it can be concluded that SIM is defined as a system that provides information that is used to support operations, management, and decision-making within an organization or company.

Hospitals

The definition of a hospital according to (Law of the Republic of Indonesia Number 17 of 2023 concerning health), is a health service institution that provides individual health services in a complete manner that provides inpatient, outpatient, and emergency services. It is also stated in Article 2 that the Hospital is organized based on Pancasila and is based on human values, ethics and professionalism, benefits, justice, equal rights and anti-discrimination, equity, patient protection and safety, and has a social function.

Hospitals established by the Central Government and Regional Governments as referred to in Article 2 of the Regulation of the Minister of Health of the Republic of Indonesia Number 44

of 2009, must be in the form of a Technical Implementation Unit from an Agency in charge of the health sector, or a certain Agency with the management of a Public Service Agency or a Regional Public Service Agency in accordance with the provisions of the laws and regulations of the Regulation of the Minister of Health Number 3 of 2020. Based on Law of the Republic of Indonesia Number 17 of 2023, hospitals have the following functions:

1. Hospitals provide individual health services in the form of specialists and/or subspecialists.
2. The hospital provides basic health services.
3. Hospitals carry out educational and research functions in the health sector.
4. Hospitals maintain good hospital governance and clinical governance.

Hospital Management Information System

The hospital management information system according to Permenkes 82 of 2013 concerning the hospital management information system is an information communication technology system that processes and integrates the entire flow of the hospital's service process in the form of a coordination network, reporting and administrative procedures to obtain information appropriately and accurately, and is part of the Health Information System. SIMRS is a set or activity and procedures that are organized and interrelated and interdependent and designed in accordance with the plan in an effort to provide accurate, timely and necessary information to support the process of management functions and decision-making in providing health services in hospitals (Windarti and Nadya, 2023).

Information Systems Audit

Auditing is a factual method of creating evidence from guaranteeing the statement that has been described and the criteria are determined, which obtains results to evaluate which include questions of circumstances or actions with weighty transactions, as well as communicating to actors, users, and executors who have an interest in achieving results (Ginanjar et al., 2026). There are several activities that include information system audits that have stages such as planning, then conducting field inspections, reporting, and most importantly conducting follow-ups. Integrity, reability, convidentiality, system availability, efficiency, and effectiveness, as well as audits of data sources, security perspectives, audits of mechanisms, data files, and changes in programs are some of the perspectives examined in conducting information system testing (Winarto, 2022).

Data Security

Data security is an effort to protect and guarantee data confidentiality, data integrity, and data availability. Information system security is a very important part to ensure the integrity and quality of the information that will be generated. Data and information need to be protected from carelessness, intentionality and technical and ethical issues that are expected to damage, eliminate or hinder the distribution process (Garfinkel and Lipford, 2014).

RESEARCH METHODS

This study uses a qualitative approach with the literature review method which aims to identify, analyze, and synthesize scientific findings related to information system audits in hospitals in improving the security and integrity of patient data. Literature review was chosen because it allows researchers to conduct conceptual mapping, critical evaluation, and integration of previous research results in a comprehensive and structured manner (Snyder, 2019). This

method is also relevant to examine the development of information systems audit standards, With this approach, the research does not generate field data, but relies on an in-depth analysis of credible and up-to-date scientific literature.

The focus of this research is the protection of health data which is classified as sensitive data and vulnerable to security breaches (Kruse et al., 2017). In addition, data integrity is a crucial aspect in healthcare because errors or manipulation of patient data can have a direct impact on patient safety (Alharthi et al., 2019). Therefore, information systems audits are positioned as a strategic control mechanism to ensure regulatory compliance, system effectiveness, and medical data protection. The data sources in this study are in the form of secondary data obtained from indexed international and national journal articles (Scopus, Web of Science, SINTA, and Google Scholar), conference proceedings, academic books, and official standards and guidelines related to information system auditing and health data security. Literature inclusion criteria include: (1) publications in the 2016–2026 range, (2) discussing information systems audits, health data security, or patient data integrity, and (3) being available in full text. The keywords used include "information system audit", "hospital information system", "data security", "data integrity", and "electronic health records security".

Data analysis techniques are carried out with content analysis and thematic synthesis to identify patterns, research gaps, and strategic recommendations from various sources studied (Elo & Kyngäs, 2008). Each article is analyzed based on the audit variables, the framework used (e.g. COBIT or ISO 27001), the type of security risk identified, and the impact on the integrity of patient data. The results of the analysis are then categorized into key themes, such as IT governance, access control, risk management, and regulatory compliance evaluation. This approach allows for the development of a comprehensive conceptual framework for how information systems audits contribute to improving the security and integrity of patient data in hospitals.

RESULTS AND DISCUSSION

Research Results

Based on the literature search carried out, several articles that are in accordance with this research are presented in the following table.

Table 1. Research Results

No	Name (Year)	Title	Research Methods	Research Results
1	Ullah et al. (2024)	Blockchain-enabled EHR access auditing: Enhancing healthcare data security	Development of a blockchain-based EHR audit system with integration of Purpose-Based Access Control (PBAC) and smart contracts	The research resulted in an EHR audit system with immutable blockchain-based trail audits, PBAC integration for access legitimacy verification, audit log creation, and the provision of data-driven insights to strengthen access security and reduce unauthorized entries.
2	Mejía-Granda et al. (2025)	A method and validation for auditing e-Health applications based on reusable software security requirements specifications	Systematic literature review, preparation of security catalogs based on ISO/IEC/IEEE 29148:2018, and validation through OpenEMR audits using the SEC-AM method	Audits of OpenEMR identified vulnerabilities such as DDoS, XSS, JSONi, and CMDi, with a security compliance rate of 66.97% ("Secure" category). Security catalogs are proven to be feasible and effective for improving the security of health software.

3	Dogiye et al. (2025)	Assessing Data Integrity and Security in Healthcare Information Management Practice	Descriptive analytical review dan expert-practice synthesis	Threats to data integrity and security include human error, legacy systems, insecure data migration, weak access controls, and cyberattacks. Effective interventions include data governance framework, role-based access control, data encryption, routine trail audits, staff training, device management, and incident response plans.
4	Setiatin & Azmi (2024)	Analysis of Patient Data Security Aspects in the Implementation of EMR at Hospital X Bandung	Qualitative research with analysis based on the CIA Triad	EMR implementations still have vulnerabilities: the absence of auto-logout, encryption, multi-factor authentication, and trail audits; backup is still manual; Periodic training and audits have not been carried out. A comprehensive security framework is needed for continuous data protection.
5	Rasyad & Lubis (2025)	Hospital Patient Data Security Evaluation to Achieve SDGs 3.8.1 "Good Health and Wellbeing"	Evaluative qualitative research (interviews, observations, documentation, thematic analysis)	Hospitals have implemented VPNs, access restrictions, and dashboard monitoring. However, there have been no routine audits, specific evaluation indicators, minimal staff training, and cryptography techniques have not been optimal. Blockchain-based encryption, formal incident response protocols, periodic audits, and comprehensive training are recommended.
6	Shojaei et al. (2024)	Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review	Systematic Literature Review	Identify HIS security technologies such as IoT, blockchain, mobile health, cloud computing, and a combination of technologies. Emphasizes three key aspects of security: secure access control, data sharing, and data storage, as well as the challenges in each.
7	Adnyana et al. (2025)	Audit of Hospital Management Information Systems Based on The COBIT 4.0 Framework	Audit using COBIT 4.0 framework (PO, AI, DS, ME) and maturity level analysis	The audit results in an assessment of the Maturity Level of the hospital's IT system which is the basis for recommendations to improve the effectiveness and efficiency of services to support the hospital's mission as a Regional Public Service Agency.
8	Lestari et al. (2024)	Improving Healthcare Patient Data Security: An Integrated Framework Model for EHR from a Legal Perspective	Mixed-method (normative analysis of laws and empirical studies of health facilities)	Gaps in the implementation of Permenkes No.24/2022 and Law No.27/2022 were found, especially in small facilities. Developed an ISU-EMR framework based on the CIA Triad and HCI to improve data protection while maintaining the usability of the EMR system.

Discussion

An audit of information systems in hospitals is a systematic and structured evaluation process of information technology infrastructure, security policies, control mechanisms, and data management practices that aims to ensure the security, integrity, confidentiality, and availability of patient data. In the healthcare sector, patient data is categorized as highly sensitive because it encompasses personal identification information, medical history, diagnostic results, treatment records, and financial data, all of which are closely linked to individual privacy rights

and the continuity of clinical services. Any breach, manipulation, or loss of such data can directly affect patient safety, institutional reputation, and compliance with legal and regulatory frameworks. As emphasized by Dogiye et al. (2025), the increasing digitalization of hospital information systems significantly expands the attack surface for cyber threats, thereby making systematic auditing an essential component of organizational risk management. Through comprehensive audits, hospitals are able to identify weaknesses in access control, network security, system configuration, and user management practices before these vulnerabilities are exploited.

According to Ron Weber in *Information Systems Auditing* (1999), information systems auditing is defined as the process of collecting and evaluating evidence to determine whether an information system safeguards assets, maintains data integrity, and supports the achievement of organizational goals effectively and efficiently. This conceptualization remains highly relevant in contemporary hospital settings, where information systems must not only function reliably but also align with governance standards, ethical principles, and strategic healthcare objectives. The findings in this literature review reinforce Weber's perspective by demonstrating that audits function not merely as technical inspections or vulnerability detection tools, but also as strategic instruments for strengthening internal controls, enhancing accountability, and fostering continuous improvement in data security governance. By integrating audit results into policy revision, staff training, and technological upgrades, hospitals can build a more resilient digital environment that supports high-quality healthcare delivery while ensuring compliance with both national regulations and international best practices.

The various studies in this study show that the threat to the security and integrity of patient data is multidimensional. Dogiye et al. (2025) identified a number of major threats, including human error, the use of legacy systems, insecure data migration processes, weak access controls, and increasing complexity of cyberattacks. The threat is not only technical, but also closely related to the managerial and cultural aspects of the hospital organization. This finding is strengthened by Shojaei et al. (2024) through a systematic literature review which confirms that health information systems (HIS) face serious challenges in three main aspects, namely secure access control, data sharing mechanisms, and data storage. These three aspects are interrelated and form an integrated security ecosystem; Weaknesses in one aspect have the potential to open a gap for data breaches to occur.

At the implementation level, these various vulnerabilities are reflected in the practice of managing hospital information systems. Setiatin and Azmi (2024), through a CIA Triad-based analysis of one of the hospitals in Bandung, found a number of significant weaknesses, such as the unavailability of the auto-logout feature, the lack of data encryption, the absence of multi-factor authentication, and the absence of a structured audit trail. In addition, the data backup process is still carried out manually and security training for staff has not been carried out regularly. Similar findings were presented by Rasyad and Lubis (2025) who evaluated the security of patient data in the context of achieving SDGs 3.8.1. Although the hospitals studied have implemented VPNs, access restrictions, and monitoring systems through dashboards, routine audits have not been conducted consistently, security evaluation indicators have not been standardized, staff training is still limited, and the application of cryptographic techniques has not been optimal. This condition shows that there is a gap between the safety standards that should be applied and the actual practice in the field, especially in hospitals in Indonesia.

These implementation gaps not only have an impact on the technical aspect, but also have significant legal implications. Lestari et al. (2024), through a mixed-method approach that

combines legal normative analysis and empirical studies, found that many health facilities, especially small-scale ones, have not fully implemented the provisions of the Minister of Health Regulation No. 24 of 2022 concerning Electronic Medical Records and Law No. 27 of 2022 concerning Personal Data Protection. In response to these conditions, this study developed an ISU-EMR framework based on the principles of the CIA Triad and Human-Computer Interaction (HCI), with the aim of improving data protection without neglecting the usability aspect. This approach is in line with the view of Whitman and Mattord (2018) who affirm that effective information security must balance technical, managerial, and user experience dimensions in order to be implemented consistently in the organization.

In an effort to strengthen audit practices, various technological frameworks and approaches have been developed. Adnyana et al. (2025) used the COBIT 4.0 framework which includes the domains of Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME) to evaluate hospital management information systems. The results of the audit in the form of maturity level assessments are the basis for the preparation of recommendations to improve the effectiveness and efficiency of IT services. The use of COBIT is considered appropriate because it provides a comprehensive and scalable IT governance structure. On the other hand, Mejía-Granda et al. (2025) developed an approach based on the ISO/IEC/IEEE 29148:2018 security catalog validated through an audit of OpenEMR applications using the SEC-AM method. The audit identified vulnerabilities such as Distributed Denial of Service (DDoS), Cross-Site Scripting (XSS), JSON Injection (JSONi), and Command Injection (CMDi), with a security compliance rate of 66.97% which falls into the "Secure" category. These findings suggest that a documented security standards-based approach can be an effective and applicable audit instrument.

Furthermore, Ullah et al. (2024) presented innovations through the development of a blockchain-based Electronic Health Record (EHR) audit system that integrates Purpose-Based Access Control (PBAC) and smart contracts. This system results in an immutable trail audit, so that every access record cannot be changed or deleted by any party. The PBAC mechanism ensures that access to patient data is only granted based on legitimate purposes and is automatically verified by the smart contract, thus minimizing the potential for unauthorized access. Rasyad and Lubis (2025) also recommend the implementation of blockchain-based encryption as a strategy to strengthen hospital data security. The decentralized, transparent, and manipulation-resistant characteristics of blockchain make it a potential solution in strengthening audit trails and health data access verification mechanisms (Ekblaw et al., 2016).

In addition to technological innovation, the literature consistently emphasizes the importance of nontechnical interventions as an integral part of data security strategies. Dogiye et al. (2025) recommend the implementation of data governance frameworks, role-based access control, data encryption, periodic trail audits, staff training, device management, and incident response plans as complementary policy packages. The recommendations affirm that advanced technology will not be optimal without the support of competent human resources and structured organizational procedures. This is in line with the view of Von Solms and Van Niekerk (2013) who stated that information security is an issue that is not only technical, but also related to human factors and organizational culture, so it requires an integrated approach between technology, policies, and user behavior.

Overall, the synthesis of eight studies in this study provides a comprehensive overview of information system audit practices in hospitals. First, threats to the security and integrity of patient data are complex and multidimensional, encompassing technical, managerial, legal, and human behavioral aspects (Dogiye et al., 2025; Shojaei et al., 2024; Setiatin & Azmi, 2024).

Second, various audit approaches, both framework-based such as COBIT (Adnyana et al., 2025) and security catalog-based (Mejía-Granda et al., 2025), have proven effective in identifying vulnerabilities and formulating measurable improvement recommendations. Third, technological innovations such as blockchain (Rasyad & Lubis, 2025) open up new opportunities in strengthening trail audits and access control. Fourth, compliance with national regulations is still a challenge, especially for health facilities with limited resources (Lestari et al., 2024). Therefore, strengthening information system audits in hospitals needs to be carried out holistically and sustainably through the integration of standardized frameworks, the adoption of relevant technologies, the fulfillment of legal obligations, and the systematic increase in human resource capacity.

CONCLUSIONS AND SUGGESTIONS

Based on the results of the literature synthesis, it can be concluded that information system audits in hospitals play a strategic role in ensuring the security, integrity, and availability of patient data amid the increasing complexity of cyber threats and regulatory demands. Threats to patient data are multidimensional, including technical, managerial, legal, and human aspects, requiring a comprehensive and structured audit approach. Various frameworks such as COBIT and ISO/IEC/IEEE-based security standards have proven effective in identifying vulnerabilities and providing measurable remediation recommendations, while technological innovations such as blockchain offer potential solutions in strengthening trail audits and access controls. However, there is still a gap between ideal security standards and implementation practices in the field, especially in health facilities with limited resources, so that strengthening information security governance is an urgent and sustainable need.

The suggestions that can be given are for hospitals to implement periodic information system audits with reference to standardized and measurable frameworks, as well as ensure alignment with national regulations related to the protection of personal data and electronic medical records. In addition to strengthening technical aspects such as encryption, multi-factor authentication, and an integrated audit trail system, hospital management also needs to increase the capacity of human resources through continuous information security training and the formation of a security awareness culture. Governments and relevant stakeholders are also advised to provide technical guidelines and implementation support for small-scale hospitals to meet the established safety standards. With a holistic and collaborative approach, information system audits in hospitals are expected to be able to become a strategic instrument in increasing public trust and the overall quality of health services.

REFERENCES

Book:

Garfinkel, S., & Lipford, H. R. (2014). *Usable security: History, themes, and challenges*. Morgan & Claypool Publishers.

Ginanjar, Y., Judijanto, L., & Susilawati, M. (2026). *Auditing*. PT. Sonpedia Publishing Indonesia.

Weber, R. (1999). *Information Systems Auditing: The Big Questions*. University of Queensland.

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security (6th ed.)*. Cengage Learning.

Winarto, W. W. A. (2022). *Audit sistem informasi*. Penerbit NEM.

Windarti, S., & Nadya, A. (2023). *Implementasi sistem informasi manajemen rumah sakit (SIMRS)*. Penerbit NEM.

Article in journal:

Adnyana, G. F., Wasita, R. R., & Trinoto, A. A. (2026). Audit of Hospital Management Information Systems Based on The COBIT 4.0 Framework. *Faktor Exacta*, *18*(4). http://dx.doi.org/10.30998/faktorexacta.v18i4.28720.

Ahmad, A., Hastuti, J., & Hijriatin, M. (2025). Data Security Analysis in Electronic Health Information Systems. *Journal Informatic, Education and Management (JIEM)*, *7*(1), 1-11. https://doi.org/10.61992/jiem.v7i1.107.

Alhadi, B. I. (2022). Sistem Informasi Manajemen (Sim) Sebagai Sarana Pencapaian E-Government. *Jurnal Stie Semarang (Edisi Elektronik)*, *14*(2), 184-195. https://doi.org/10.33747/stiesmg.v14i2.564

Alharthi, A., Krotov, V., & Bowman, M. (2017). Addressing barriers to big data. *Business Horizons*, *60*(3), 285-292. https://doi.org/10.1016/j.bushor.2017.01.002

Asih, H. A., Indrayadi, I., Soraya, S., & Khairunnisa, K. (2024). Evaluasi Keamanan Data Pasien Pada Rekam Medis Elektronik Dengan Systematic Literature Review. *Jurnal Ilmiah Fifo*, *16*(2), 104-110. http://dx.doi.org/10.22441/fifo.2024.v16i2.001.

Dogiye, E. L., Adebisi, A. A., & Biobelemeye, G. G. (2025). Assessing data integrity and security in healthcare information management practice. *International Journal Of Health Records & Information Management (IJHRIM)*, *8*(1).

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of advanced nursing*, *62*(1), 107-115. https://doi.org/10.1111/j.1365-2648.2007.04569.x.

Krisdiyawan, R. D., & Kuswantoro, R. H. (2017). Audit keamanan sistem informasi pada rs mata dr. Yap yogyakarta menggunakan framework cobit 5. *Jurnal Ilmiah Manajemen Informasi dan Komunikasi*, *1*(1), 8-15. https://doi.org/10.56873/jimik.v1i1.44.

Lestari, A. Y., Misran, M., Raharjo, T., Annas, M., Riskanita, D., & Prabandari, A. P. (2024). Improving healthcare patient data security: an integrated framework model for electronic health records from a legal perspective. *Law Reform*, *20*(2), 329-352. https://doi.org/10.14710/lr.v20i2.56986.

Mardiah, A., Na'am, J., & Kurnia, H. (2018). Perancangan Aplikasi Customer Relationship Management (CRM) untuk Meningkatkan Layanan Pelanggan pada Toko Lusi Ana Gorden Lubuk Alung Berbasis Web dengan Menggunakan PHP DAN MYSQL. *Jurnal KomtekInfo*, *5*(1). https://doi.org/10.35134/komtekinfo.v5i1.11.

Mejia-Granda, C. M., Fernández-Alemán, J. L., de Gea, J. M. C., & Garcia-Berna, J. A. (2025). A method and validation for auditing e-Health applications based on reusable software security requirements specifications. *International Journal of Medical Informatics*, *194*, 105699. https://doi.org/10.1016/j.ijmedinf.2024.105699.

Munthe, B. O., Amalia, F., & Cholissodin, I. (2019). Pengembangan Sistem Informasi Penilaian dan Evaluasi Kinerja Karyawan Dengan Metode Weighted Product Berbasis Web (Studi Kasus: UB Guest House). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*(9), 9095-9104.

Rasyad, M. F., & Lubis, R. L. (2025). Hospital Patient Data Security Evaluation to Achieve SDGs 3.8. 1 "Good Health and Wellbeing". *Enrichment: Journal of Multidisciplinary Research and Development*, *2*(12), 1572-1579.

Setiatin, S., & Azmi, A. R. (2024). Analysis of Patient Data Security Aspects in the Implementation of Electronic Medical Records (EMR) at Hospital X Bandung. *International Journal Prima Husada Health (IJPHH)*, *1*(2), 173-180.

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. *Computers*, *13*(2), 41. https://doi.org/10.3390/computers13020041.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, *104*, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., ... & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon*, *10*(16). https://doi.org/10.1016/j.heliyon.2024.e34407

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004.

Conference/proceeding:

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). *A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data.* Paper presented at the 2nd International Conference on Open and Big Data (OBD), Vienna, Austria.