GREENATION PUBLISHER
IJPHS:
International Journal of Psychology and Health Science
+62 812 1046 7572 http://greenpub.org greenation.info@gmail.com
DOI: https://doi.org/10.38035/ijphs.v3i3

Analysis of Electronic Medical Record Security Aspects in Maintaining Patient Data Confidentiality at Hospital X in Bandung City

Sri Rahayu[1], Sali Setiatin[2]
[1]Politeknik Piksi Ganesha, Jawa Barat, Indonesia, rahayuuus09@gmail.com
[2]Politeknik Piksi Ganesha, Jawa Barat, Indonesia, salisetiatin@gmail.com

Corresponding Author: rahayuuus09@gmail.com[1]

Abstract: The implementation of the Electronic Medical Record (EMR) system at Hospital X is a strategic step to enhance the efficiency and quality of healthcare services. This study aims to evaluate data security aspects of the EMR system, focusing on access security, data integrity, and system availability. A descriptive qualitative method was used to explore patient data protection practices. The results indicate that the hospital has implemented role-based access control, audit trails, and user activity monitoring. However, several shortcomings were identified, such as the absence of a regular password change policy, lack of two-factor authentication, and infrequent system security testing. In terms of availability, the system is supported by 24-hour vendor services, although technical challenges such as network disruptions and hardware limitations remain. This study recommends strengthening security policies, conducting regular staff training, and improving technological infrastructure to ensure optimal patient data protection and service effectiveness.

Keyword: Security aspects, Electronic medical records, Patient data confidentiality

.

INTRODUCTION

Advancements in information technology have driven major transformations across various sectors, including data protection. These technological developments have significantly changed how data is safeguarded, particularly in the healthcare sector. Risks such as data breaches, misuse, and cyberattacks demand the implementation of more robust and well-organized security systems. Hospitals, as primary healthcare institutions, bear the responsibility of maintaining the confidentiality of patient data, which often involves highly sensitive medical information (Turkstani et al., 2025). One form of digital service transformation in hospitals is the implementation of Electronic Medical Records (EMR). This system allows for the digital and integrated recording and management of patient information (Kemenkes, 2022). Healthcare workers can access patient data quickly and accurately, which positively impacts the speed of diagnosis and clinical decision-making. EMRs have also been shown to reduce patient waiting times (Nafiza & Ulfah, 2024). It is widely accepted that the implementation of EMR systems enhances the quality of hospital services. Several studies have demonstrated that EMR usage significantly accelerates healthcare workflows and increases patient satisfaction (Latipah et al., 2021). Furthermore, EMRs reduce the risk of errors caused by manual documentation and provide a comprehensive health history to support continuous care (Ikawati, 2024).

In addition to efficiency, data security is a critical aspect of EMR implementation. Regulation of the Minister of Health No. 24 of 2022 mandates that healthcare facilities ensure the confidentiality, integrity, and availability of patient data according to standardized formats, metadata, and access based on general consent. This principle aligns with the CIA triad (Confidentiality, Integrity, Availability), which forms the foundation of information security systems (Bozic, 2023). Data protection in EMR systems must also comply with Law No. 27 of 2022 concerning Personal Data Protection, which emphasizes responsibility and caution in data management, including the application of encryption, multi-layered authentication, and audit trails (Republik Indonesia, 2022). A study by Liu et al. (2024) indicated that EMR systems remain vulnerable to disruptions and cyberattacks.

Based on preliminary observations at Hospital X in Bandung, the EMR system has been integrated through the Hospital Information System (SIMRS), featuring personal accounts, role-based access control, and activity logging. However, there are still shortcomings, such as the absence of two-factor authentication, digital signatures, routine password update policies, and limited internal audits. Although basic security features like confidentiality, integrity, and access control are in place, patient data protection needs to be comprehensively improved (Tiorentap & Hosizah, 2020).

A previous study by Suhariyono et al. (2025) at UPT Karangploso Health Center demonstrated security system implementation through access restrictions and long-term data availability. Meanwhile, this current research is conducted by the researcher at Hospital X in Bandung during its transitional phase of EMR implementation, offering a more up-to-date and relevant context regarding data security dynamics. Therefore, this study aims to evaluate the security level of the EMR system at Hospital X.

METHOD

This study employs a qualitative descriptive method to explore the implementation of security aspects in the Electronic Medical Record (EMR) system for safeguarding patient data confidentiality at Hospital X, Bandung City. This method was selected to provide an in-depth understanding of policies, operational practices, and the perspectives of system implementers regarding patient data protection (Pradono et al., 2018). Data were collected through in-depth interviews with key informants involved in EMR security, direct observation of data protection practices in the field, and analysis of hospital policy documents and technical information security system records. The interviews aimed to gather insights on informants' views regarding data protection systems, leakage risks, and mitigation strategies, while observations were used to verify the alignment between stated procedures and actual practices (Harahap, 2020).

Subjects were selected purposively and consisted of the Information Technology team (IT–Hospital X), medical records officers (MR–Hospital X), and inpatient administrative staff (ADM–Hospital X), all of whom have knowledge and direct responsibility for EMR security (Murdiyanto, 2020). Data analysis was conducted thematically in three stages: data reduction through transcription and categorization of relevant information into themes such as data security and protection strategies; data presentation in narrative and visual forms to facilitate analysis of inter-theme relationships; and drawing conclusions that were validated through data triangulation from interviews, observations, and supporting documentation (Abdussamad, 2021).

RESULT AND DISCUSSION

Result

Overview of Hospital X

Hospital X, located in Bandung, began transitioning from a manual system to an Electronic Medical Record (EMR) system in early 2024 to improve patient data management. Although some services are still operated manually, the hospital is actively developing its IT infrastructure and providing staff training to support this transition. This initiative is expected to accelerate the digitalization of healthcare services while enhancing the security and efficiency of medical information management.

Confidentiality Aspect in Electronic Medical Record (EMR) Data Security

Confidentiality is a crucial aspect of EMR security at Hospital X, considering the highly sensitive and private nature of medical data. Several measures have been implemented, including:

1. Authentication System Using Username and Password

Each EMR user at Hospital X is required to use a personal username and password to access patient data. An administrative staff member explained:

"Every EMR user at Hospital X is required to have a personal username and password to access patient data. This ensures that only authorized personnel can enter the system." (ADM–Hospital X)

However, the passwords do not have an expiration policy and are only changed voluntarily by users:

"We do provide usernames and passwords for all users, but currently there is no rule for periodic password changes. Passwords are only updated if users feel the need or decide to do so voluntarily." (IT–Hospital X)

This condition potentially lowers data security, especially since the system has yet to implement two-factor authentication, which remains a gap that needs to be addressed.

2. Access Rights Based on Job Position

The allocation of access rights is vital for maintaining EMR data security. At Hospital X, user access rights are structured based on job positions to ensure that each user can only access information relevant to their role and responsibilities. As stated by a medical record officer:

"At Hospital X, access rights are differentiated by job position. For instance, doctors have special access different from nurses, as do admin staff. The medical record menus and features accessible by nurses are not necessarily the same as those for doctors. For example, doctors can access both inpatient and outpatient data, while nurses only access specific features needed for their care tasks." (MR–Hospital X)

The IT team added that access is also determined based on medical necessity:

"Data access is based on users' medical responsibilities. For example, registration staff can only view basic data such as BPJS number, national ID, and administrative information, while doctors and nurses can view more detailed medical data relevant to their roles." (IT–Hospital X)

This specific access arrangement helps protect patient medical records while also ensuring smooth healthcare services at Hospital X.

3. Access Management and Third-Party Involvement

Managing access to EMR data is essential not only for internal hospital staff but also for third parties involved in system maintenance. Hospital X has strict policies regarding third-party access to protect patient confidentiality. As stated by the IT team:

"Any third-party access, such as by vendors or consultants, must first receive formal approval from the hospital. Without permission, third parties are not allowed to access any documents or patient medical data." (IT–Hospital X)

In addition to obtaining approval, close monitoring is conducted to ensure third-party access is limited to necessary system areas only:

"The hospital constantly monitors third-party access and restricts their permissions only to areas required for maintenance or troubleshooting purposes. This prevents unauthorized access and safeguards data integrity." (IT–Hospital X)

These policies on access management and third-party control are essential efforts by Hospital X to ensure EMR data security in line with standards and regulations.

4. Physical and Environmental Security

Physical and environmental security includes managing physical access to system areas and monitoring the surroundings to prevent unauthorized data access. According to the IT team:

"The medical records room and EMR system access areas are restricted and can only be accessed by authorized personnel. These rooms are equipped with security locks and limited access to prevent unauthorized entry." (IT–Hospital X)

Environmental monitoring is also implemented with CCTV:

CCTV constantly monitors activities in the medical records room. This serves as a preventive measure to detect and immediately address suspicious activities." (IT–Hospital X)

The use of computers to access EMR is strictly regulated:

"Computers in the medical records room must not be left logged in when not in use, and staff are not allowed to write down passwords at their desks to prevent unauthorized access." (IT–Hospital X)

5. Staff Implementation and Compliance

The implementation of EMR data security policies at Hospital X depends heavily on user compliance. The IT team stated that staff had received briefings on Standard Operating Procedures (SOP), although formal training sessions are not yet held regularly. In general, staff members hold positive views of the EMR system. One respondent noted:

"We consistently follow SOPs for managing medical record data, including maintaining confidentiality of usernames and passwords, and not leaving computers logged in when unattended. So far, no data confidentiality breaches have occurred at Hospital X." (MR–Hospital X)

Integrity Aspect in Electronic Medical Record (EMR) Data Security

The integrity aspect in information security refers to the accuracy and completeness of data. Integrity means that a patient's medical information must not be altered, deleted, or added without proper authorization and clear documentation.

1. Audit Trail Mechanism

Hospital X has implemented an audit trail system in the EMR application to monitor all user activities within the system. With this audit trail, every change made to patient data is recorded, including the identity of the user who made the change, the time, and the type of action taken.

"Every activity in the EMR system is recorded automatically. So, if any data changes occur, we can trace who made the changes and when." (IT–Hospital X)
The audit trail is crucial to ensure that all data changes are verifiable and to prevent misuse of access to patient medical information.

2. Restriction of Data Editing Rights

Hospital X also applies role-based access restrictions, including permissions to create, edit, or delete data.
"I can only input patient identity data, such as name and address. The medical content can only be accessed and modified by doctors and nurses." (ADM–Hospital X) "Medical record staff only handle data entry and maintenance; they do not modify diagnoses or medical actions." (MR–Hospital X)
Access rights are strictly regulated to ensure that only specific personnel can modify medical record information, according to their job functions.

3. Protection Against Unauthorized Modification

To prevent illegal or unauthorized modifications of patient data, regular system audits are conducted. Although no serious incidents have occurred so far, continuous monitoring remains a priority.
"We routinely monitor activity logs. So far, there have been no reports of data integrity violations, but prevention is still essential." (IT–Hospital X)
his monitoring is supported by a system that limits access based on user privileges.

4. Procedures for Data Correction or Revision

If data entry errors are discovered, correction procedures must go through formal reporting to ensure changes are verified and do not compromise the integrity of the medical record.
"If there's a typo or data error, we report it to a supervisor, and a correction form must be filled out. So, all changes are officially recorded." (MR–Hospital X)
This procedure also reinforces accountability for every data change within the EMR system, as all corrections are properly documented through the audit system.

Availability Aspect in Electronic Medical Record (EMR) Data Security

The availability aspect refers to the extent to which EMR data can be quickly and easily accessed by authorized personnel whenever needed, without significant disruptions. Hospital X implements various measures to ensure the optimal availability of the EMR system so that patient services can continue smoothly.

1. EMR System Availability

The EMR system operates 24/7 to support continuous patient care, especially in the emergency department, inpatient wards, and outpatient clinics.
"The system must always be on standby. Staff in all units can access patient data whenever needed." (ADM–Hospital X)

2. Vendor Support

The hospital collaborates with a vendor who provides technical support and is responsible for the EMR application infrastructure. In case of serious technical issues, the vendor is contacted immediately for quick resolution.
"We work with a vendor for system support. If there are problems on the application side, we usually report them directly, and they assist either remotely or with a technical visit. The

system wasn't developed in-house, so for major updates or bugs, the vendor handles those directly." (IT–Hospital X)

3. System Maintenance and Data Backup

Regular maintenance is conducted, including daily backups to prevent data loss and ensure quick recovery if disruptions occur. In the event of issues with patient EMR data, the hospital coordinates directly with the vendor to ensure proper data recovery. The vendor is responsible for performing daily backups and recovery processes, helping to maintain data security and availability.

"Regarding patient EMR data backups, if a problem arises, we immediately coordinate with the vendor, as they are responsible for daily backups." (IT–Hospital X)

4. Incident Handling and Backup Systems

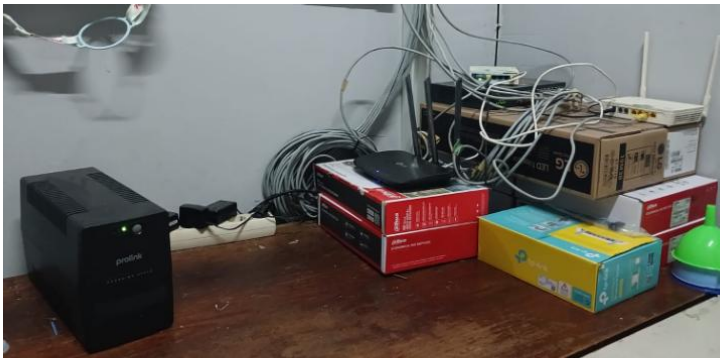

Figure 1. Server Room at Hospital X

Figure. 1. Standard procedures are in place to address system disruptions, including the use of backup servers and Uninterruptible Power Supplies (UPS) to ensure the system remains operational during recovery.

"If there's a power outage or network disruption, we have backup servers and UPS in place so the system remains accessible. If the EMR system still cannot be accessed, we immediately contact the vendor to diagnose the issue and analyze whether it's related to the network, server, or third-party services such as BPJS." (IT–Hospital X)

Additionally, the incident response process includes reporting issues to the appropriate authorities to ensure prompt resolution and system restoration.

Discussion

Analysis of Electronic Medical Record (EMR) Data Security in Terms of Access Security

Access management for the EMR system at Hospital X utilizes personal usernames and passwords to protect patient data. However, passwords are not changed routinely and are only updated at the user's discretion, which poses a security risk. This finding aligns with research by Ardianto et al. (2024), which states that without a periodic password change policy, systems are vulnerable to cyberattacks such as credential theft and unauthorized access. In addition to using usernames and passwords, Hospital X has not yet implemented two-factor authentication (2FA), which is a weakness in the EMR security system. A study by Wardani et al. (2024) at the Islamic Hospital of Jakarta Sukapura found that storing usernames and passwords in browsers and using default passwords by staff created security vulnerabilities. That study recommended implementing two-factor authentication and periodic password updates to strengthen EMR system security.

International research by Liu et al. (2024) also highlighted that cloud-based centralized hospital EMR systems are highly susceptible to attacks such as denial-of-service (DoS) and unauthorized internal access. They proposed a consortium blockchain-based scheme, data encryption, and attribute-based access control to enhance the protection of patient information. Furthermore, Kuo et al. (2017) emphasized the importance of role-based access control and multi-level authentication to prevent data breaches in hospitals. This is supported by findings from Zhang et al. (2024), which showed that implementing advanced encryption in combination with smart contracts in EMR systems can effectively ensure the confidentiality, integrity, and availability of data in hospital environments.

The access rights in the EMR system at Hospital X are customized according to users' roles and responsibilities to ensure data access only aligns with their duties. The IT team regularly reviews these settings to prevent excessive access, including managing limited access for vendors and third parties. Physical security is also enforced by securing the server room with locks and CCTV monitoring. This aligns with the Ministry of Health Regulation (Kemenkes, 2022) on Electronic Medical Records, particularly Articles 29 through 31, which regulate EMR security aspects. Article 29 emphasizes the principles of confidentiality, integrity, and data availability for authorized parties. Article 30 regulates healthcare workers' access rights in managing EMR data. Article 31 allows the use of electronic signatures for verification and security purposes, although it is not mandatory. In the case of Hospital X, digital signatures had not yet been implemented during this study. (Kemenkes, 2022).

Staff compliance in implementing security policies is also a crucial factor in maintaining EMR system access. Although staff have received socialization regarding EMR management practices, formal training specifically focused on EMR security has not been conducted regularly. Nevertheless, staff generally remain consistent in maintaining the confidentiality of usernames and passwords and follow proper system usage procedures, such as not leaving logged-in computers unattended. Research by Omidah & Yunengsih (2025) also highlights similar issues, where several staff members failed to log out before leaving their computers and had not changed passwords regularly, increasing the risk of unauthorized access by unapproved individuals.

Analysis of Electronic Medical Record (EMR) Data Security in Terms of Data Integrity

The aspect of integrity within the Electronic Medical Record (EMR) system at Hospital X is crucial for maintaining the accuracy and completeness of patient data. The audit trail system, which records every user activity including the identity of the user and the time of changes is a fundamental component in ensuring that data remains intact and protected from unauthorized modification. This reflects the principle of integrity in information security, which demands protection against unauthorized changes and the ability to verify every data modification. Through an automated audit trail, the system provides transparency over all activities, reducing the risk of data misuse. In addition, role-based access restrictions are implemented to safeguard the integrity of EMR data. Only doctors and nurses are authorized to modify medical records, while medical record officers are responsible for data entry and maintenance. This structure minimizes the risk of unauthorized data changes. These findings are consistent with research by Wardani et al. (2024), which concluded that role-based access control is highly effective in preserving data integrity and reducing the risk of illegal modifications within EMR systems.

Regular system monitoring through user activity logs demonstrates Hospital X's commitment to maintaining data integrity. Even though no security breaches have occurred so far, continuous monitoring represents a proactive effort to anticipate potential risks. Ardianto et al. (2024) also emphasized the importance of system monitoring as a preventive measure to secure EMR data, particularly for the early detection of suspicious activity or unauthorized modifications. Finally, the implementation of formal procedures for data correction, which include reporting and the use of correction forms, reinforces accountability and ensures that every change is officially recorded. This approach helps maintain the integrity of medical records and prevents data manipulation that could compromise the validity of patient medical information.

Analysis of Electronic Medical Record (EMR) Data Security in Terms of System Availability

The availability aspect of the system is crucial for the smooth operation of the EMR at Hospital X with the EMR system running 24 hours a day, medical and administrative staff can access patient data at any time, especially in critical units such as the emergency department and inpatient wards. This aligns with the principle of availability, which emphasizes the importance of fast and reliable data access to support uninterrupted healthcare services. The hospital collaborates with an external vendor or system partner responsible for technical support and application infrastructure. In the event of serious technical issues, the vendor is contacted immediately to address the problem either remotely or through on-site visits.

Since the system is developed by an external partner, all updates and bug fixes fall under the vendor's responsibilities. This approach helps reduce the risk of data breaches while ensuring that the system remains consistently available to support optimal and continuous healthcare service delivery. These practices are consistent with findings from Day & Subekti (2024), who emphasized that system partners hold both legal and technical responsibility for maintaining the security and availability of EMR data, particularly in managing data breach incidents.

CONCLUSION

This study shows that the implementation of the Electronic Medical Record (EMR) system at Hospital X has incorporated various security mechanisms to protect patient data, particularly in terms of access control, data integrity, and system availability. Access management through personal usernames and passwords, along with role-based access control, has been applied to ensure confidentiality and prevent unauthorized access. However, some shortcomings remain, such as the absence of periodic password changes and the lack of two-factor authentication (2FA), which increases access security risks. In terms of data integrity, the use of audit trails and role-based access restrictions help ensure the accuracy and completeness of medical records.

This is further supported by regular user activity monitoring and formal procedures for data correction, enhancing accountability. System availability is maintained through technical support provided by the vendor, allowing the EMR system to be accessed reliably 24/7 in support of hospital operations. Nevertheless, ongoing improvements in security are necessary particularly through the implementation of two-factor authentication, regular password updates, routine security training for staff, and enhanced physical protection of server rooms. With continuous evaluation and improvement, supported by active collaboration between the hospital and the system provider, the EMR system at Hospital X is expected to operate more securely, effectively, and in compliance with applicable regulations.

REFERENCES

Abdussamad, Z. (2021). *Metode Penelitian Kualitatif*. Syakir Media Press.

Ardianto, E. T., Sabran, & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X. *RAMMIK : Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan*, *3*(2), 18–30.

Bozic, V. (2023). Confidentiality, Integrity and Availibility in hospital. *Research Proposal*.

Day, S. A. S., & Subekti, R. (2024). Pertanggungjawaban Penyedia Sistem Rekam Medis Elektronik Dari Partner System Terhadap Kebocoran Data. *Demokrasi : Jurnal Riset Ilmu Hukum, Sosial Dan Politik*, *1*(3), 92–101.

Harahap, N. (2020). *Penelitian kualitatif*. Wal Ashri Publishing.

Ikawati, F. R. (2024). Efektivitas Penggunaan Rekam Medis Elektronik Terhadap Peningkatan Kualitas Pelayanan Pasien di Rumah Sakit. *Ranah Research : Journal of Multidisciplinary Research and Development*, *6*(3), 288–298.

Kemenkes, R. I. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis*. Kementerian Kesehatan Republik Indonesia .

Kuo, T.-T., Kim, H.-E., & Machado, L. O.-. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *J Am Med Inform Assoc*, *24*(6), 1211–1220.

Latipah, T., Solihah, S., & Setiatin, S. (2021). Pengaruh Rekam Medis Elektronik Terhadap Peningkatan Efektivitas Pelayanan Rawat Jalan Di Rumah Sakit X. *Cerdika: Jurnal Ilmiah Indonesia*, *1*(10), 1422–1434.

Liu, G., Xie, H., Wang, W., & Huang, H. (2024). A secure and efcient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. *Journal of Cloud Computing: Advances, Systems and Applications*, *13*(44), 1–13.

Murdiyanto, E. (2020). *Penelitian kualitatif: Teori dan aplikasi disertai contoh proposal*. Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LP2M) Universitas Pembangunan Nasional "Veteran" Yogyakarta Press.

Nafiza, S. R., & Ulfah, A. (2024). Pengaruh Rekam Medis Elektronik Terhadap Efisiensi Pelayanan Kesehatan Poli Obgyn Di Rumah Sakit X. *Jurnal Ilmiah Multidisipliner (JIM)*, *8*(6).

Omidah, & Yunengsih, Y. (2025). ANALISIS DAMPAK KEAMANAN DATA PASIEN PADA SISTEM REKAM MEDIS ELEKTRONIK DI RUMAH SAKIT X. *Journal of Medical Record Student (JMeRS)*, *3*(1), 83–88.

Pradono, J., Soerachman, R., Kusumawardani, N., & Kasnodihardjo. (2018). *Panduan Penelitian dan Pelaporan Penelitian Kualitatif*. Lembaga Penerbit Badan Penelitian dan Pengembangan Kesehatan.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Suhariyono, U. S., Ikawati, F. R., & Afifah, N. (2025). Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso. *Jurnal Manajemen Informasi Kesehatan Indonesia*, *13*(1), 72–78.

Tiorentap, D. R. A., & Hosizah. (2020). Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP. *Prosiding 4 SENWODIPA*.

Turkstani, H. A., Almutawah, F. N., AlZamel, N. A., Alshammari, M. Z., Alhamadi, A. A., Algharbi, M. T., Alsuayri, A. M., Gong, M. B., Alqahtani, J. S., Alnemer, A. F., & Aljuwayed, N. H. (2025). Privacy and Confidentiality in Healthcare: Best Practices for Protecting Patient Information. *Journal of Healthcare Sciences*, *5*(1), 49–54.

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

Zhang, J., Guo, R., Shi, Y., & Tang, W. (2024). An anti-impersonation attack electronic health record sharing scheme based on proxy re-encryption and blockchain. *Mathematical Biosciences and Engineering*, *21*(6), 6167–6189