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

Analysis of Patient Data Security and Privacy in Electronic Medical Record Systems in Hospital X

Sali Setiatin[1], Ervien Agus Jakaria[2], Nadia Rizki Pratami[3]
[1]Politeknik Piksi Ganesha, Bandung, Indonesia, salisetiatin@gmail.com
[2]Politeknik Piksi Ganesha, Bandung, Indonesia, ervienagus55@gmail.com
[3]Politeknik Piksi Ganesha, Bandung, Indonesia, nadiarizky59@gmail.com

Corresponding Author: ervienagus55@gmail.com[2]

Abstract: The development of digital technology has had a significant impact on the world of healthcare, especially in terms of patient data management, which is now turning to Electronic Medical Records (RME). RME is expected to be a mainstay solution to improve efficiency, accuracy, and ease of access to patient data between various health facilities. In Indonesia, the One Health Data initiative from the Ministry of Health plays a crucial role in this data integration process. However, the digitization of health information also raises new problems, especially related to the protection of sensitive patient personal data. This study aims to review the extent to which security and privacy aspects have been implemented in the RME system, particularly in Hospital X. This research uses a qualitative approach through observation, in- depth interviews, and document studies. The results of the study revealed that although the RME system is equipped with a simple authentication system using usernames and passwords, the security practices implemented are still less than optimal. There is still a lack of weak password use, a reluctance to change passwords periodically, and the absence of a special Standard Operating Procedure (SOP) that regulates the security and confidentiality of patient data. In addition, user awareness of the importance of protecting data is also still relatively low. These findings show that the successful implementation of RME does not only depend on the availability of technology, but also requires strengthening administrative policies and increasing understanding of cybersecurity among medical personnel. Therefore, a comprehensive strategy is needed to ensure the protection of patient data on an ongoing basis.

Keywords: Electronic Medical Records, Information Security, Data Privacy, Systems

INTRODUCTION

The transformation of healthcare services at both global and national levels heavily depends on the implementation of Electronic Medical Records (EMRs). The digitalization of health information through EMRs is a key factor in replacing manual recording systems to ensure smooth patient data exchange, in alignment with the One Health Data program initiated by the Ministry of Health of the Republic of Indonesia (Kemenkes RI, 2022). This initiative aims to consolidate all patient data from various healthcare facilities to improve

efficiency, accuracy, and secure accessibility for authorized parties. For relevant articles, refer to keywords such as "Medical Records," "Patients," and "Hospitals." Research findings indicate that data security for patients in EMR usage has been adequately implemented (Yunengsih, Y., 2025).

Despite the numerous benefits of EMR implementation, significant challenges remain, particularly regarding the security and privacy protection of patient data (Santhi, 2025). Hospitals, as providers of comprehensive health services, are obliged to maintain EMR documentation from admission to discharge, covering outpatient care, inpatient care, and emergency services (Minister of Health Regulation No. 24 of 2022). EMRs are digital documents containing patient identity data, examination results, treatments, medical procedures, care details, and all other services received by the patient throughout the treatment process.

Unfortunately, the increasing number of healthcare data breaches indicates that many healthcare facilities still lack adequate information security management systems. Weak authentication, insufficient encryption systems, and the absence of consistent audit trails can create opportunities for illegal access and data manipulation (Wijayanti et al., 2024). A literature review by Asgiani et al. (2022) highlights the importance of implementing cryptographic technologies, firewalls, and access controls to maintain data integrity and confidentiality. However, in practice, many hospitals in Indonesia have yet to adopt basic security principles such as non-repudiation and segmented user access.

National regulations such as Law No. 27 of 2022 concerning Personal Data Protection have outlined principles of consent, transparency, and control over personal data, including medical records. Furthermore, Minister of Health Regulation No. 11 of 2017 on Patient Safety also mandates that hospitals maintain the confidentiality of patient information as part of service quality indicators. However, the implementation of these regulations is still inconsistent across hospitals. Thus, security and confidentiality must be maintained by both internal and external factors. A similar situation was found at Hermina Arcamanik Hospital, where several documents were found missing outside the storage area (Fauzi, M. R., Fauzia, R. M., & Setiatin, S., 2021). Several legal analyses also point out weaknesses in enforcing data protection mechanisms and digital oversight, including the lack of standardized security systems based on ISO/IEC 27001 (Mandey, 2025). Without strengthening technical, administrative, and user behavior aspects, EMRs could become a vulnerable point in the digital transformation of healthcare services. On the other hand, EMRs have the following disadvantages: risks of malware and system errors, potential data entry or editing mistakes, vulnerability to hacking, and heavy dependence on electricity availability (Putri, S., & Gunawan, E., 2022).

Medical records serve as a basis for patient care and therapy, legal evidence in court, support for research and education activities, healthcare service payment processes, and the preparation of health statistics (Maulani, A. N., Ridwan, A. N., Hidayati, M., & Susanto, A., 2021). Based on the above background, this study aims to analyze the implementation of security and privacy systems in the use of Electronic Medical Records (EMRs) at Hospital X. The research will cover technical aspects such as encryption and authentication, administrative aspects such as data protection policies, and user behavior aspects such as staff compliance with security procedures. The results of this study are expected to provide a comprehensive overview and evidence-based recommendations for improving health information security in hospitals.

METHOD

The research method used in this study is a qualitative research method, according to Sugiyono (2022), the qualitative method isThe research method, which is based on the philosophy of postpositivism, is used to research on the condition of natural objects, where the researcher is the key instrument, the data collection technique is triangulation (a combination of observation, interviews, and documentation), and data analysis is inductive. This approach was chosen in order to comprehensively understand the application of patient data security and privacy in electronic medical record systems, both from a technical perspective and from a user perspective. This design is suitable for answering research questions related to policy effectiveness, technical implementation, and practitioners' views in the field through a triangulative method.

This study was conducted using a studied population where the population was taken from all health workers and medical record workers working at Hospital X, who had used an electronic medical record system for at least one year.

Where the sample selection technique used is purposive sampling non-probability, with inclusion criteria in the form of officers who have the right to access patient data through the RME system.

Collection was carried out through interviews, observations, and documentation. This research procedure begins with the administrative preparation stage and permit application, followed by the collection of qualitative data collection through in-depth interviews that are recorded and transcribed. The informants in this study were 3 hospital officers, including 2 medical record officers, 1 IT officer . All data was collected over a three-month period, while still adhering to the ethical principles of the research, including informed consent, confidentiality of identity, and the right of participants to withdraw at any time.

RESULT AND DISCUSSION

The research conducted revealed several key findings regarding the level of security and privacy experienced by patients in relation to the electronic medical record (EMR) system at Hospital X. Based on the interviews that were carried out, the following results were obtained:

1. Evaluation of Patient Data Security in the Use of Electronic Medical Records at the Hospital

This can be reviewed from the aspect of confidentiality, which refers to efforts to protect patients' personal information from being accessed by unauthorized parties. Since medical records contain private and sensitive data, only medical personnel or authorized individuals with legal permission are allowed to access them. Confidentiality is essential because it ensures the protection of data and information from threats—whether internal or external—especially from those who are not entitled to access it. Therefore, the data and information stored in the electronic medical record system will be safeguarded against misuse and unauthorized dissemination.

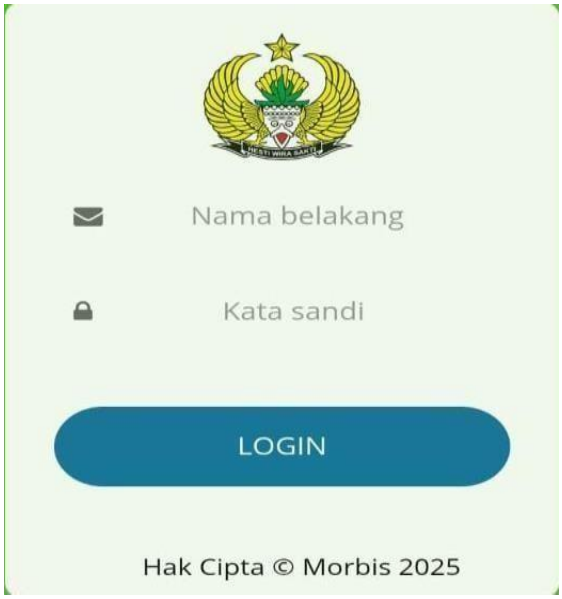

Figure 1. Electronic Medical Record (EMR) Login Menu

Based on the research findings discussing personal data protection in the use of electronic medical records, information was obtained through interviews with respondents as follows:

> According to Respondent 1, (2025): the information contained in the medical record is considered confidential and is protected using a username and password.

Based on the results of assessments and interviews, it was found that the EMR system requires the use of a username and password for access. This finding aligns with previous studies stating that usernames and passwords in EMRs function as proof that an individual has authorized access to the system and aim to prevent unauthorized access. Although the use of passwords is an essential part of maintaining system security, there are still vulnerabilities—particularly related to users' tendency to choose weak passwords. Interviews with several staff members revealed that the passwords used in the EMR system do not yet incorporate special characters. The following are excerpts from the interviews with respondents:

> According to Respondent 1 (2025), the passwords used in the system do not yet include special characters.

with an IT staff member:

> According to Respondent 2 (2025), the use of special characters in passwords depends on the individual staff member; some use them, while others avoid them due to the tendency to forget.

> According to Respondent 3 (2025), special characters should ideally be used in passwords; however, in practice, this is often challenging because users frequently complain about forgetting them. The more complex the password, the more difficult it becomes to remember.

Regularly changing usernames and passwords aims to anticipate the possibility of such information being discovered by unauthorized parties. According to the findings from the interviews, the following are several responses from IT team members. Below are excerpts from the interviews with members of the IT team:

> According to Respondent 3 (2025), there should be a routine schedule for changing usernames and passwords; however, in practice, this is difficult to implement.

Respondents, two admitted that they had not regularly changed their usernames and passwords. Regularly updating usernames and passwords is essential to minimize the risk of unauthorized individuals gaining access to sensitive data. In addition to changing login credentials, the implementation of an automatic log-out feature can also be used to help maintain patient data confidentiality. The following are excerpts from the interviews with the respondents:

> According to Respondents 1 and 2, the automatic log-out feature is already available in the system.

Based on the interview findings, two respondents stated that the system is equipped with an automatic log-out feature, which was confirmed by the IT department. This is in line with previous studies indicating that one method of protection is through an automatic log-out system—where if no activity is detected within 30 (thirty) minutes, the system will automatically log the user out. The following are several responses from the respondents:

> According to Respondent 3 (2025): “That feature is already available, where if the system is left idle for about 30 minutes, it requires a refresh and will automatically log out. To access it again, the user must re-enter their username and password.”

After conducting a series of interviews, it was found that the EMR system is already equipped with an automatic log-out feature. However, the waiting period before the system logs out automatically—30 (thirty) minutes of inactivity—is considered suboptimal. The security of patients’ personal information is not limited to system protection alone, but also concerns who is authorized to access the information and for what purposes. It is crucial to have a monitoring mechanism that safeguards patient data privacy in EMRs, ensuring that only authorized parties can view the information.

2. To further examine the security of patient data related to the use of Electronic Medical Records (EMR) systems for medical information at Hospital X, particularly from the perspective of integrity. Integrity means ensuring the security of data so that no changes occur without the approval of authorized parties.

> According to Respondent 1, 2025: “In its implementation, the medical records of discharged patients can no longer be edited, and the data cannot be deleted. A patient’s medical history must be preserved and must not be removed.”

> Respondent 2, 2025: “Independent data editing is still possible within a 2x24 hour timeframe. However, for now, if an error occurs, corrections cannot be made directly and must follow predetermined procedures. Nevertheless, if an error is discovered in the field, editing can be done on the spot with the approval or knowledge of a supervisor.”

Based on the interview results, it was revealed that the E-MR system has a feature that allows for modifications, namely an editing function. In general, deletion is not permitted, and altering information in electronic medical records is not allowed. Therefore, additional protective measures are needed to prevent unauthorized deletion or editing of data. Hospital X applies a time limit of 2 x 24 hours for data modification, in accordance with regulations. The interview results with respondents are presented below:

> Respondent 3, 2025: "Regarding this matter, the system has actually been set up so that patient data, such as in the discharge summary and anamnesis, cannot be edited after the patient is discharged, in accordance with applicable regulations. However, in practice, there is still a possibility that the data can be modified."

Interpretation of the statement supported by the IT team indicates that the E-MR system at Hospital X allows for patient data editing. Based on interviews with relevant parties, if there is an error in the medical record, doctors are allowed to make corrections. However, for substantial changes, revisions must be carried out in accordance with the regulations and procedures applicable within the hospital.

Research findings focusing on the aspect of integrity indicate that the level of protection for patient information using Electronic Medical Records at Hospital X is considered good. One contributing factor is the editing feature, which is restricted to specific personnel according to the access rights granted based on their responsibilities, authority, and roles in healthcare services. Furthermore, deletion of patient data in the system is not permitted. Therefore, any modification of information in the electronic medical record must follow official procedures to ensure the security and integrity of patient data.

Furthermore, an analysis was also conducted on the authentication aspect of the E-MR system. Authentication plays a crucial role in ensuring secure access to patient information by verifying the legitimacy of a user's identity before allowing access to the system. Several authentication methods that can be implemented include the use of passwords, PINs, or biometric technology. Based on the results of observations and interviews, the system at Hospital X has implemented user IDs and passwords as a means of verifying that staff members have authorized access to the E-MR system.

Furthermore, efforts to maintain the security of private data from the verification side are also supported by the implementation of electronic signatures. In the implementation of electronic medical records in healthcare facilities, digital signatures are used as proof of document authenticity and the validity of the signer's identity. Based on the research conducted at Hospital X, it was found that the implementation of digital signatures has been running optimally as part of strengthening the security and authentication system within the electronic medical records.

The interview results serve as evidence of this:

> Respondent 1, 2025: The electronic signature system is already in place, where the signing process is carried out by scanning a signature that is integrated with the doctor's username and password. In this case, the doctor simply enters an identification code or doctor ID as a form of authentication to validate the electronic signature.

> Respondent 2, 2025: The electronic signature system is indeed available; however, its implementation does not yet include patients. For signatures required from patients, the manual method—direct handwritten signatures—is still being used.

This statement is supported by information from the IT department. The following is an excerpt from the interview with a member of the IT team:

> Respondent 3, 2025: Regarding this matter, the system is already available; however, in the context of electronic medical records, regulations concerning electronic signatures have not yet been specifically defined. There are no clear provisions outlining whether signatures should be done through scanning, barcode generation, or other methods. Nevertheless, an authorized institution responsible for regulating and issuing electronic signature certificates is already in place.

Electronic signatures are digital information linked or attached to other electronic documents and serve as a means of verifying and authenticating identity. According to Article 11 of the Law on Information and Electronic Transactions (UU ITE) of 2008, electronic signatures have the same legal power as manual signatures, provided that several specified requirements are met. One of the main requirements for an electronic signature to be legally valid is its use through an official electronic certification service provider. At Hospital X, this system has begun to be implemented as part of efforts to strengthen the information system and protect patient data.

Based on research on the authentication variable, it was found that the security system for patient information in the use of Electronic Medical Records at Hospital X includes the implementation of electronic signatures by certified care-providing doctors. This reinforces the legal validity of recording and managing electronic medical records. However, the study also found that, in the case of patients, the document signing process is still carried out manually, meaning that the implementation of electronic signatures has not yet been fully applied across all service elements.

3. In-Depth Review of Patient Health Data Security Based on the Aspect of Availability

The availability aspect of patient data security refers to the assurance that information can be accessed by authorized parties at any time and from any location when needed. In the context of Electronic Medical Records (EMRs), the information storage system must be capable of ensuring the continuous security, integrity, confidentiality, and availability of patient data.

EMRs serve as the primary communication tool in healthcare services, so their availability must be guaranteed at all times and accessible without delay. The system should be capable of displaying previously stored medical information efficiently, without significant delays.

The research conducted at Hospital X shows that the aspect of availability has been implemented effectively. Electronic Medical Record data can be accessed through the hospital's internal network by authorized users who have appropriate access rights. This supports the smooth delivery of medical services, as patient information can be retrieved quickly when needed.

The following is a quotation from an interview with one of the respondents regarding the implementation of the availability aspect in the EMR system at Hospital X:

> Respondent 1, 2025: Access to the EMR can only be carried out within the hospital environment using the hospital's internal internet network.

This statement from the respondent is supported by the results of an interview with the IT team, who provided the following explanation:

> Respondent 3, 2025: Access cannot be performed outside the hospital's network and environment; it can only be done through the hospital's VPN, which has been configured by the IT team. Therefore, access is not openly available to everyone.

Based on the interview results, it was found that access to the Electronic Medical Records (EMR) system can only be made through the hospital's internal internet network. Every staff member with login access can easily use the EMR system; however, access is restricted to a designated network. This is in line with the Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions, which states that every electronic system provider must operate systems in accordance with applicable standards. This provision ensures that patient service information can only be accessed by authorized personnel, in accordance with access rights and defined limitations.

Research findings on the availability aspect of the EMR system show that patient data security has been implemented fairly well. This is evident from the restriction of system access only through the hospital's internal network or via a VPN configured by the IT team. Such restrictions serve as preventive measures aimed at protecting patient information from potential unauthorized access.

In addition, healthcare professionals also find it easy to access patient service information, although there is a minor issue in that all departments (poli) can view patient data, which may raise concerns about access control boundaries.

4. Review of Medical Information Security at Hospital X Based on Access Control in the Implementation of Electronic Medical Records

Access control is a critical component of how an information system manages user permissions. This step is taken to ensure that only authorized personnel can access and use the health information system. Access control helps protect patient data through the use of usernames and passwords to manage EMR users and assigns different access rights based on the user's job role, authority, and responsibilities.

The following are the results of interviews conducted with respondents regarding access rights in the EMR system:

> Respondent 1, 2025: Access rights are managed by the IT team, as they are based on proposals from the relevant departments.

The following is supporting evidence for that statement, obtained from the response of an IT division respondent, as revealed in the IT team interview excerpt:

> Respondent 3, 2025: Access restrictions are managed through the use of usernames and passwords.

Referring to the interview results, the access rights system at Hospital X is managed through the assignment of usernames and passwords. These accounts are created by the IT team based on requests from each respective department. From discussions with informants, it was revealed that the EMR interface appears the same for all users, although the access rights differ. The following is an excerpt from the interview with a respondent:

> Respondent 2, 2025: The EMR interface is the same.

According to the response from a respondent working in the IT team, the visual layout of the EMR system is generally the same for all users; however, access to certain menus is restricted. This means not all features can be used by every user. The following is an excerpt from the interview with the IT team:

The menu interface in the system is uniform for all users; however, there are specific access settings based on each user's role. For example, medical record officers are only granted permission to view data without editing access, while doctors have the authority to both view and edit information within the system.

Following the interviews, it was found that all menus in the EMR system appear uniform. To restrict who can access certain features, the EMR system is configured so that unauthorized users cannot utilize them. This study also revealed that the system's user interface has not been fully tailored to reflect the varying levels of access rights among users. Although each user has different access limitations based on their role, the available menu visuals remain largely the same.

Based on the assessment of the access control aspect, it can be concluded that patient data security is implemented through an access restriction mechanism that uses a combination of usernames and passwords. This mechanism is applied according to the duties, authority, and responsibilities of each system user.

The results of this study in this aspect show that although the entire menu display in the EMR system appears identical for all users, the system has been configured so that certain features can only be accessed by individuals with responsibilities corresponding to their roles. This indicates that access control emphasizes functional restrictions within the system rather than visual menu differentiation.

5. Patient Data Protection Review Based on the Aspect of Nonrepudiation

The nonrepudiation aspect in information security refers to the system's ability to accurately log all user activities, including any modifications or manipulations of data within the system. This principle ensures that every user action can be tracked and cannot be denied at a later time. This aligns with the provisions of Government Regulation of the Republic of Indonesia No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, which mandates the availability of audit trails for all activities in electronic systems to serve the purposes of supervision, legal compliance, validation, as well as auditing and dispute resolution processes.

Based on research and interviews conducted, it was found that the EMR system at Hospital X is equipped with a user activity logging feature. This feature records every interaction made by users, allowing identification of who made changes, when the changes were made, and what type of action was performed. Thus, the system has incorporated the nonrepudiation principle as part of its patient data protection efforts.

The following is an excerpt from an interview with one of the respondents regarding the implementation of nonrepudiation access in the EMR system:

> Respondent 1, 2025: The system is equipped with a log recording feature, where all data accessed or opened by users is automatically recorded in the activity log.

This statement is further supported by information from the IT team. The following is an excerpt from the interview with a respondent from the information technology department:

> Respondent 3, 2025: In this case, we can view log records that capture details of user access and any changes made. The current medical record system includes an audit trail feature, which allows us to track data that has been deleted. Therefore, we can identify who deleted the data and understand why the action was taken.

Based on the study conducted on the non-repudiation variable, it can be concluded that the issue of patient health data privacy security in the use of Electronic Medical Records has been addressed. This is because, from the perspective of non-repudiation, the system already records user activity history related to data access. As a result, it is possible to trace who has viewed or modified patient information.

CONCLUSION

In terms of confidentiality, the security of patient information in the electronic medical record (EMR) system has implemented a login mechanism using usernames and passwords. However, there are still weaknesses in user practices, where some staff members do not regularly update their passwords or use secure combinations such as numbers, letters, and special characters. In addition, there is no specific Standard Operating Procedure (SOP) regulating security and confidentiality policies for the electronic medical record system.

For the integrity aspect, the EMR system is equipped with an editing feature that can only be accessed by authorized personnel based on their duties and responsibilities in the hospital. Any data modification in the system cannot be done directly but must follow established procedures. This aims to ensure that patient data integrity is maintained and to prevent unauthorized manipulation.

In terms of authentication**,** the electronic medical record system has implemented certified electronic signatures for attending physicians as a form of validation and legal authentication of the electronic documents generated. However, findings show that forms requiring patient signatures are still completed manually, indicating that the system has not yet fully adopted digital processes in all areas.

Regarding availability, the EMR system supports good accessibility by limiting access solely through the hospital's internal internet network or a VPN configured by the IT team. This measure is intended to maintain patient data security. Healthcare personnel can access patient information with ease, although all departments currently still have access to patient service data without restriction by service unit.

In terms of access control, the EMR system restricts user access through an authentication mechanism involving usernames and passwords, tailored to each individual's role, responsibility, and authority. Although the visual layout of the system menus appears uniform, access control is enforced by disabling specific features for unauthorized users, ensuring that only authorized personnel can access and utilize certain functions according to their roles.

REFERENCES

Asgiani, P., Suryawati, C., & Agushybana, F. (2022). A literature review: Security aspects in the implementation of electronic medical records in hospitals. *Media Ilmu Kesehatan, 10*(2), 161–166.

Efri, T. A., 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.

Fauzi, M. R., Fauzia, R. M., & Setiatin, S**.** (2021). Kerahasiaan dan Keamanan Rekam Medis di Rumah Sakit Hermina Arca Manik. *Politeknik Piksi Ganesha, Bandung, Cendekia: Jurnal Ilmiah Indonesia, 9*(1), 1161–1169.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO.

Kementerian Kesehatan Republik Indonesia. (2017). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 11 Tahun 2017 tentang Keselamatan Pasien Rumah Sakit*. Jakarta: Kemenkes RI.

Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik*. Jakarta: Kemenkes RI.

Mandey, A. W. (2025). Legal analysis of patient privacy violation in electronic medical records and its implications for health data protection in Indonesia. *Jurnal Multidisiplin Sahombu, 5*(2), 589–594.

Maulani, A. N., Ridwan, A. N., Hidayati, M., & Susanto, A. (2021). Analisis Pengimplementasian Pendistribusian Berkas Rekam Medis Pasien Rawat Jalan Di Rumah Sakit X Bandung. *Jurnal Ilmiah Perekam dan Informasi Kesehatan Imelda (JIPIKI), 6*(2), 174–182.

Putri, S., & Gunawan, E. (2022). Pelaksanaan Retensi Pada Masa Peralihan Rekam Medis Manual Ke Rekam Medis Elektronik (RME) Di Klinik Utama Cahaya Qalbu. *Media Bina Ilmiah, 16*(11), 7687–7696.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)*. Jakarta: Kementerian Komunikasi dan Informatika.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Jakarta: Kementerian Komunikasi dan Informatika.

Santhi, N. N. P. P. (2025). Patient data privacy challenges in electronic health systems: A juridical analysis of medical information protection in Indonesia. *West Science Law and Human Rights, 3*(1), 1–8.

Wijayanti, D., Ujianto, E. I. H., & Rianto, R. (2024). Uncovering security vulnerabilities in electronic medical record systems: A comprehensive review of threats and recommendations for enhancement. *JITEKI (Jurnal Ilmiah Teknik Elektro dan Komputer Indonesia), 10*(1).

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.