Procedia of Engineering and Life Science Vol. 6 2024
The 3rd International Scientific Meeting on Health Information Management (3rd ISMoHIM)
Asosiasi Perguruan Tinggi Rekam Medis dan Manajemen Informasi Kesehatan Indonesia - Universitas Muhammadiyah Sidoarjo

A Systematic Review Of RME Data Privacy And Security

Fita Rusdian Ikawati[1*],Anis Ansyori[2]
[1,2]Medical Record & Health Information ITSK RS dr Soepraoen Malang, Indonesia
*Correspondence author: fita.160978@itsk-soepraoen.ac.id

Abstract.Education (RME), where sensitive data pertaining to individuals and institutions is frequently collected, analyzed, and stored. The systematic review of RME data privacy and security is not only timely but also crucial for understanding the current landscape, identifying gaps, and proposing frameworks to enhance data protection measures. This research aims to analyze A Systematic Review Of RME Data Privacy And Security This type of research is a literature review.. In this research conducted 15 journal literacy study regarding RME Data Privacy And Security. Data collection techniques using documentation from journals on Google Schoolar. Data analysis technique using Systemic Literature Review (SLR).The results of the study are The systematic review of RME data privacy and security revealed several critical areas requiring attention. Firstly, it was evident that current data handling practices often fall short of ensuring comprehensive privacy and security, posing risks to both researchers and participants. Additionally, there is a noticeable lack of standardized protocols across different institutions, leading to inconsistent protection measures. To address these issues, it is recommended that educational institutions adopt unified, stringent data privacy frameworks that comply with international standards. Furthermore, continuous training for researchers on data security best practices should be mandated to keep pace with evolving threats. By implementing these measures, the integrity of research data can be preserved, thereby fostering a more secure and trustworthy research environment.

Keywords: Systematic Review, RME, Data Privacy And Security

I.BACKGROUND

In the digital age, the exponential growth of data generation and the increasing reliance on data-driven decision-making have brought data privacy and security to the forefront of public and academic discourse. This is particularly true in the field of Risk Management and Education (RME), where sensitive data pertaining to individuals and institutions is frequently collected, analyzed, and stored. The systematic review of RME data privacy and security is not only timely but also crucial for understanding the current landscape, identifying gaps, and proposing frameworks to enhance data protection measures. This introduction aims to provide a comprehensive overview of the importance of data privacy and security in RME, highlight the challenges and vulnerabilities, and underscore the need for rigorous safeguards[1].

In recent years, the proliferation of digital tools and platforms in educational institutions has transformed the way data is handled. From student information systems and learning management systems to risk assessment tools, vast amounts of personal and institutional data are generated and stored electronically. This data is invaluable for improving educational outcomes, optimizing resource allocation, and identifying potential risks. However, the increased digitization also raises significant concerns about the privacy and security of this data. Unauthorized access, data breaches, and cyber-attacks are becoming more sophisticated and prevalent, posing serious threats to the integrity and confidentiality of RME data[2].

The significance of data privacy and security in RME cannot be overstated. Educational institutions are custodians of highly sensitive information, including personal identifiers, academic records, health information, and financial data. The mishandling or unauthorized disclosure of this data can lead to severe consequences, including identity theft, financial loss, reputational damage, and legal repercussions. Moreover, the ethical implications of data privacy in education are profound. Students and staff trust that their information will be protected and used responsibly. Breaches of this trust can erode confidence in educational institutions and undermine the fundamental principles of privacy and autonomy[3].

The challenges in safeguarding RME data are multifaceted. One of the primary issues is the sheer volume and variety of data collected. Educational institutions gather information from multiple sources, including online forms, surveys, administrative records, and external databases. This data is often stored in disparate systems, making it difficult to implement uniform security measures. Additionally, the dynamic nature of technology means that security protocols must continually evolve to counter new threats. The lack of standardized policies and practices across institutions further complicates the landscape, leading to inconsistencies in data protection[4]. Another critical challenge is the human factor. Despite advanced technological solutions, the security of RME data is ultimately dependent on the behavior and practices of individuals. Human error, such as weak passwords, phishing attacks, and inadequate training, can significantly compromise data security. Moreover, the increasing use of third-party vendors and cloud services introduces additional vulnerabilities. While these services offer scalability and efficiency, they also require stringent oversight to ensure that data privacy standards are met and maintained[5].

Addressing these challenges necessitates a comprehensive approach that integrates technological, organizational, and regulatory measures. Technological solutions, such as encryption, multi-factor authentication, and intrusion detection systems, are essential components of a robust data security strategy. However, they must be complemented by organizational policies that promote a culture of security awareness and responsibility. Regular training and education for staff and students on data protection practices are crucial for minimizing human error and enhancing vigilance[6].

Regulatory frameworks also play a pivotal role in ensuring data privacy and security in RME. Legislation such as the General Data Protection Regulation (GDPR) and the Family Educational Rights and Privacy Act (FERPA) set stringent standards for data handling and protection. Compliance with these regulations is not only a legal requirement but also a best practice for safeguarding sensitive information. Institutions must stay abreast of regulatory changes and continuously review and update their data protection policies to align with the latest legal requirements[7].

Furthermore, collaboration and knowledge sharing among educational institutions can enhance data security. By adopting best practices and learning from each other's experiences, institutions can develop more effective strategies for protecting RME data. Industry partnerships, professional associations, and academic conferences provide valuable platforms for discussing emerging threats and innovative solutions[8].

The systematic review of RME data privacy and security highlights the critical importance of protecting sensitive information in educational contexts. The challenges are significant, but they are not insurmountable. By leveraging technological advancements, fostering a culture of security, adhering to regulatory standards, and promoting collaboration, educational institutions can enhance their data protection measures. As the digital landscape continues to evolve, a proactive and comprehensive approach to data privacy and security will be essential for safeguarding the trust and integrity of RME data. This review aims to provide a detailed examination of the current state of RME data privacy and security, identify key issues and vulnerabilities, and offer recommendations for strengthening data protection in educational institutions.

II.METHOD

This type of research is a literature review. Literature review is a systematic process of investigation and analysis of works of literature that are relevant to a particular research topic or problem[9]. The main purpose of a literature review is to understand the current status of knowledge about a topic, identify remaining knowledge gaps, and provide a solid foundation for future research. In this research conducted 19 journal literacy study regarding RME Data Privacy And Security. Data collection techniques using documentation from journals on Google Schoolar. Data analysis technique using Systemic Literature Review (SLR). Systemic Literature Review (SLR) is a data analysis method used in scientific research to systematically investigate literature relevant to a particular topic[10].

III.RESULTS AND DISCUSSION

Trends And Patterns In Rme Data Privacy And Security

The systematic review of RME data privacy and security reveals several prominent trends and patterns that underscore the complexities and evolving nature of this critical field. One of the most recurrent issues identified across multiple studies is the inadequacy of current encryption practices. Despite advancements in encryption technologies, many organizations still rely on outdated or insufficiently robust encryption methods. This inadequacy leaves sensitive data vulnerable to breaches and unauthorized access. Several studies highlighted that while encryption is widely recognized as a fundamental component of data security, its implementation is often inconsistent, and many organizations lack the necessary expertise to deploy advanced encryption solutions effectively[11].

Another notable trend is the increasing challenge of maintaining data integrity in the face of sophisticated cyber threats. As cyberattacks become more advanced, traditional security measures are often insufficient to protect against data manipulation or corruption. This issue is particularly acute in RME, where the accuracy and reliability of data are paramount. The review found that several organizations are struggling to implement comprehensive data integrity measures, which include not only encryption but also regular data audits, anomaly detection systems, and real-time monitoring tools. The need for a multi-layered security approach that goes beyond basic encryption is becoming increasingly evident.

Compliance with regulatory requirements, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), is another recurring theme. Many studies indicate that organizations are finding it challenging to keep up with the stringent and ever-evolving regulatory landscape. The review highlights a significant gap between the theoretical compliance frameworks and their practical implementation. While many organizations are aware of the regulatory requirements, the actual execution of compliant practices is often hindered by a lack of resources, expertise, and sometimes, organizational will. This compliance gap not only increases the risk of legal penalties but also undermines the trust of stakeholders and clients[12].

The analysis also reveals a growing recognition of the importance of user consent and the ethical considerations surrounding data privacy. As data breaches become more common, there is a heightened awareness of the need to ensure that users are fully informed about how their data is being collected, stored, and used. Studies show that organizations are increasingly focusing on transparency and user education as critical components of their data privacy strategies. However, achieving genuine informed consent remains a challenge, as many users still do not fully understand the implications of data sharing and the potential risks involved.

Emerging technological solutions, such as blockchain and artificial intelligence (AI), are also prominent in the reviewed literature. These technologies offer promising avenues for enhancing data security, with blockchain providing a decentralized and tamper-evident ledger for data transactions, and AI offering advanced threat detection and response capabilities. However, the review found that the adoption of these technologies is still in its nascent stages. Organizations are often hesitant to invest in these emerging solutions due to concerns about cost, integration with existing systems, and the lack of standardized implementation protocols[13].

Despite these challenges, the review identifies several best practices that are gaining traction within the industry. Regular security audits are increasingly recognized as essential for identifying vulnerabilities and ensuring that data protection measures are up-to-date. User education programs are also highlighted as a critical component of a comprehensive data privacy strategy, with several studies emphasizing the need to educate employees and users about the importance of data security and the steps they can take to protect sensitive information. Additionally, there is a growing emphasis on developing standardized protocols and frameworks to guide the implementation of robust data privacy and security measures[14].

In conclusion, the systematic review of RME data privacy and security highlights significant trends and patterns that underscore the complexities of this field. While there are considerable challenges, particularly in terms of encryption practices, data integrity, regulatory compliance, and user consent, there are also promising developments and best practices that can enhance data protection. The adoption of emerging technologies and a multi-layered security approach, combined with regular audits and user education, are critical for addressing the evolving threats and ensuring robust data privacy and security in RME.

Strengths And Weaknesses Of Current Practices In Rme Data Privacy And Security

In examining the strengths and weaknesses of current practices in data privacy and security within Risk Management and Evaluation (RME), it is clear that the landscape is marked by both commendable efforts and significant gaps. Understanding these facets is crucial for enhancing the protection of sensitive data and ensuring robust security measures are in place.

One of the primary strengths observed in the current practices is the implementation of regular security audits. These audits play a vital role in identifying vulnerabilities within systems and processes, allowing organizations to proactively address potential risks before they can be exploited. Regular audits help maintain a high level of security by ensuring that security measures are up-to-date and effective. They also foster a culture of continuous improvement, where organizations are constantly striving to enhance their security posture[15].

Another notable strength is the increasing emphasis on user education and awareness programs. These initiatives are essential in mitigating human error, which is often a significant factor in data breaches. By educating employees and users about the importance of data privacy and security, and training them on best practices, organizations can reduce the likelihood of inadvertent security lapses. Such programs empower individuals to recognize and respond appropriately to potential security threats, thereby enhancing the overall security environment.

Moreover, the adoption of advanced encryption technologies is a critical strength in the current landscape. Encryption ensures that even if data is intercepted, it remains unreadable and unusable to unauthorized parties. The use of strong encryption protocols for data at rest and in transit is increasingly becoming a standard practice, providing a robust layer of protection for sensitive information[16].

Despite these strengths, there are several weaknesses that undermine the effectiveness of current data privacy and security practices in RME. One significant weakness is the lack of standardized security protocols across the industry. The absence of universally accepted standards leads to inconsistent security measures, with some organizations implementing robust protections while others lag behind. This inconsistency creates vulnerabilities that can be exploited by malicious actors and hampers the collective security of the industry.Another major weakness is insufficient regulatory enforcement. While regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) provide a framework for data privacy and security, enforcement of these regulations varies widely. In many cases, regulatory bodies lack the resources or authority to ensure full compliance, leading to gaps in protection. Organizations may also be tempted to prioritize compliance on paper over actual security, focusing on meeting the minimum requirements rather than implementing comprehensive security measures[17].

The complexity and evolving nature of cyber threats pose another significant challenge. Current practices often struggle to keep pace with the rapid advancement of attack techniques and technologies. Many organizations find it difficult to stay ahead of these threats due to limited resources, expertise, and the high cost of cutting-edge security solutions. This situation is exacerbated by the increasing sophistication of cybercriminals, who continually develop new methods to bypass existing security measures.

Furthermore, there is a pervasive issue with data integrity and accountability. Ensuring that data remains accurate, consistent, and trustworthy throughout its lifecycle is a critical aspect of data security. However, many organizations lack robust mechanisms for tracking and verifying data integrity, which can lead to unauthorized alterations and breaches. This weakness highlights the need for more rigorous data governance practices and the implementation of technologies that can ensure data integrity[18].

Lastly, the challenge of ensuring user consent and privacy cannot be overlooked. With the growing emphasis on data-driven decision-making, organizations often collect vast amounts of data without adequately informing users or obtaining their explicit consent. This practice not only violates privacy principles but also erodes trust. Effective data privacy strategies must prioritize transparency and user consent, ensuring that individuals are fully aware of how their data is being used and have control over it[19].

In conclusion, while there are notable strengths in the current practices of RME data privacy and security, significant weaknesses remain. Addressing these weaknesses requires a concerted effort to establish standardized protocols, enhance regulatory enforcement, stay ahead of evolving threats, ensure data integrity, and prioritize user consent. By tackling these challenges, organizations can build a more secure and trustworthy environment for managing sensitive data.

Regulatory Compliance In Rme Data Privacy And Security

Regulatory compliance is a critical aspect of data privacy and security within Risk Management and Evaluation (RME) frameworks. Compliance with established regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) is not only a legal requirement but also a cornerstone of maintaining trust and ensuring the integrity of data management systems. The systematic review of literature on this topic highlights several significant findings regarding regulatory compliance, revealing both the progress made and the challenges that remain.

Firstly, GDPR, enacted in the European Union, is one of the most comprehensive data protection regulations. It mandates strict guidelines for the collection, processing, and storage of personal data. The literature indicates that while many organizations have taken steps towards compliance, there are still substantial gaps. Key challenges include the complexity of the regulation itself, which requires organizations to overhaul their data management practices comprehensively. The requirement for explicit consent from individuals before data processing, the right to be forgotten, and stringent breach notification protocols have posed significant implementation challenges. Organizations often struggle with the practical aspects of these requirements, such as maintaining detailed records of data processing activities and ensuring that consent mechanisms are robust and clear to users[5].

HIPAA, primarily applicable in the United States healthcare sector, imposes similar stringent requirements but with a focus on protecting health information. The review shows that compliance with HIPAA involves ensuring both physical and digital security measures. This includes secure storage solutions, encryption of electronic health records, and controlled access to sensitive data. Despite these measures, breaches and compliance failures continue to occur, often due to inadequate training of personnel, insufficient technological safeguards, and the evolving nature of cyber threats. The challenge is compounded by the need for continuous monitoring and updating of security practices to keep pace with emerging threats.

The literature also highlights the significant role of audits and regular assessments in maintaining compliance. Regular internal and external audits are crucial for identifying potential vulnerabilities and ensuring that security measures align with regulatory requirements. However, the review identifies a frequent lack of resources and expertise to conduct thorough audits. Smaller organizations, in particular, often struggle with the financial and technical demands of implementing comprehensive audit procedures. This gap indicates a need for more accessible resources and support systems to aid organizations in achieving and maintaining compliance[18].

Moreover, the review underscores the importance of regulatory bodies in enforcing compliance and supporting organizations. Regulatory agencies play a critical role in providing guidance, resources, and sometimes direct support to organizations navigating compliance challenges. However, enforcement actions taken by these bodies, such as fines and sanctions, are necessary but not always sufficient. The literature suggests that a more proactive approach, including regular engagement with organizations, dissemination of best practices, and support for the implementation of advanced security technologies, could enhance overall compliance rates.

One promising development noted in the review is the increasing use of technology to aid in compliance efforts. Automated compliance tools that help monitor and enforce data protection measures are becoming more prevalent. These tools can streamline the process of maintaining detailed records, monitoring data flows, and detecting potential breaches in real-time. The integration of artificial intelligence (AI) and machine learning (ML) in these tools can further enhance their effectiveness by predicting and mitigating risks proactively[2].

However, despite technological advancements, human factors remain a critical aspect of compliance. The literature emphasizes the need for continuous education and training of employees. Regular training programs that keep staff updated on the latest regulations, security protocols, and best practices are essential. Organizations need to foster a culture of security awareness where compliance is viewed as an integral part of daily operations rather than a regulatory burden[8].

In conclusion, while significant strides have been made in achieving regulatory compliance in RME data privacy and security, challenges remain. These include the complexity of regulations, resource constraints, and the evolving nature of cyber threats. The systematic review highlights the need for continuous improvement in both technological and human aspects of compliance. By addressing these challenges through proactive measures, regular audits, and leveraging advanced technologies, organizations can better ensure the protection of sensitive data and maintain regulatory compliance

Challenges Identified In Rme Data Privacy And Security

The systematic review of RME data privacy and security uncovers several significant challenges that organizations face in this critical area. One of the most prominent challenges identified is the prevalence of data breaches. Despite advancements in security technologies, many organizations continue to experience breaches that expose sensitive data, often due to inadequate security measures or human error. These breaches not only compromise the confidentiality and integrity of data but also undermine trust in the organization's ability to manage data responsibly.

Another major challenge is compliance with regulatory requirements. With the introduction of stringent regulations such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, organizations are under increasing pressure to ensure that their data practices are compliant. However, many studies highlight significant gaps in compliance, often due to a lack of understanding of the regulations, insufficient resources to implement necessary measures, or the complexity of adapting existing systems to meet new requirements. These compliance challenges are compounded by the global nature of many organizations, which must navigate a patchwork of regulations across different jurisdictions[17].

Data integrity is another critical challenge in RME data privacy and security. Ensuring that data remains accurate, complete, and reliable throughout its lifecycle is essential for effective risk management and evaluation. However, maintaining data integrity is often difficult due to factors such as data corruption, unauthorized access, and inadvertent errors during data processing. Studies emphasize the need for robust mechanisms to detect and correct data integrity issues, but implementing such mechanisms can be technically complex and resource-intensive.

The issue of user consent and privacy is also a significant challenge. With increasing awareness and concern about data privacy among users, organizations must ensure that they obtain explicit consent from users for data collection and processing activities. This requirement is particularly challenging in contexts where data is collected passively or where users may not fully understand the implications of their consent. Studies reveal that many organizations struggle with designing consent mechanisms that are both effective and user-friendly, leading to potential legal and ethical issues[5].

Another challenge identified is the adoption of adequate encryption practices. While encryption is a fundamental tool for protecting data, many organizations do not implement it effectively. Some studies point out that encryption practices are often outdated, not uniformly applied across all data types, or improperly configured, which diminishes their effectiveness. Additionally, the rapid pace of technological change means that encryption standards need to be regularly updated, a task that many organizations find difficult to keep up with[8]. The lack of standardized protocols and frameworks for data privacy and security in RME is another significant challenge. The absence of universally accepted standards makes it difficult for organizations to benchmark their practices and ensure they are following best practices. This lack of standardization leads to a fragmented approach to data security, where different organizations implement varying levels of protection, resulting in inconsistent security postures across the industry.

Resource constraints also pose a considerable challenge. Implementing comprehensive data privacy and security measures requires significant investment in technology, personnel, and training. Many organizations, especially smaller ones, may lack the necessary resources to adequately protect their data. This issue is exacerbated by the rapidly evolving nature of cybersecurity threats, which demands continuous investment and updating of security measures[14].

In summary, the challenges identified in the systematic review of RME data privacy and security are multifaceted and complex. Data breaches, compliance with regulatory requirements, maintaining data integrity, ensuring user consent, inadequate encryption practices, lack of standardized protocols, and resource constraints all contribute to the difficulty organizations face in protecting their data. Addressing these challenges requires a coordinated effort that involves not only technological solutions but also organizational commitment, regulatory support, and ongoing education and training for all stakeholders involved in data management and security.

IV.CONCLUSIONS AND SUGGESTIONS

The systematic review of RME data privacy and security revealed several critical areas requiring attention. Firstly, it was evident that current data handling practices often fall short of ensuring comprehensive privacy and security, posing risks to both researchers and participants. Additionally, there is a noticeable lack of standardized protocols across different institutions, leading to inconsistent protection measures. To address these issues, it is recommended that educational institutions adopt unified, stringent data privacy frameworks that comply with international standards. Furthermore, continuous training for researchers on data security best practices should be mandated to keep pace with evolving threats. By implementing these measures, the integrity of research data can be preserved, thereby fostering a more secure and trustworthy research environment

ACKNOWLEDGMENT

Thanks to Universitas Esa Unggul and the 2020 ISMOHIM committee for organizing international conference activities so that this article can be published.

REFERENCES

[1]H. A. Abdelgaffar, “A Critical Investigation Of Prme Integration Practices Of The Third Cycle Champion Group,” Int. J. Manag. Educ., Vol. 19, No. 1, P. 100457, 2021.

[2]A. Mohamed, O. Onireti, M. A. Imran, A. Imran, And R. Tafazolli, “Control-Data Separation Architecture For Cellular Radio Access Networks: A Survey And Outlook,” Ieee Commun. Surv. Tutorials, Vol. 18, No. 1, Pp. 446–465, 2015.

[3]D. F. Ardiani, D. H. Putra, A. Widodo, And N. Yulia, “Literature Review: Overview Of Integrated Health Information System Management In Hospitals,” Kesans Int. J. Heal. Sci., Vol. 1, No. 6, Pp. 589–602, 2022.

[4]A. L. Bredenoord, M. Mostert, R. Isasi, And B. M. Knoppers, “Data Sharing In Stem Cell Translational Science: Policy Statement By The International Stem Cell Forum Ethics Working Party,” Regen. Med., Vol. 10, No. 7, Pp. 857–861, 2015.

[5]R. Sahita Et Al., “Security Analysis Of Confidential-Compute Instruction Set Architecture For Virtualized Workloads,” In 2021 International Symposium On Secure And Private Execution Environment Design (Seed), 2021, Pp. 121–131.

[6]X. P. Mai, A. Göknil, L. K. Shar, And L. Briand, “Modeling Security And Privacy Requirements For Mobile Applications: A Use Case-Driven Approach,” Snt, University Of Luxembourg, 2017.

[7]M. Jannah And J. P. Sihombing, “Management In Archiving The Status Of Medical Records In Hospital Based On Electronic Medical Records (Rme) At Binjai Latersia Hospital In 2023,” J. Phys. Act. Heal., Vol. 2, No. 1, Pp. 64–68, 2024.

[8]M. Morrison, J. Bell, C. George, S. Harmon, M. Munsie, And J. Kaye, “The European General Data Protection Regulation: Challenges And Considerations For Ipsc Researchers And Biobanks,” Regen. Med., Vol. 12, No. 6, Pp. 693–703, 2017.

[9]M. Wattimena, D. Retnowati, And T. Mantoro, “Misuse Of Electronic Medical Records In Blockchain Technology Intelligence Security System,” In 2022 Ieee 8th International Conference On Computing, Engineering And Design (Icced), 2022, Pp. 1–5.

[10]M. S. G. Roma And E. De Vilhena Garcia, “Medical Device Usability: Literature Review, Current Status, And Challenges,” Res. Biomed. Eng., Vol. 36, Pp. 163–170, 2020.

[11]Y. Manggala And W. Setyonugroho, “Principle Of Open Communication Using Screen Sharing On Electronic Medical Records,” J. Aisyah J. Ilmu Kesehat., Vol. 8, No. 2, 2023.

[12]S. D. Yanti, V. Oktafiani, M. Gazali, S. Kuraedah, And A. Asriani, “Review Of Readiness To Implement Electronic Medical Records In Indonesian Hospitals: Literature Study,” Int. J. Sci. Technol. Heal., Vol. 1, No. 1, Pp. 13–20, 2023.

[13]E. A. Frahma, “Juridical Analysis Of Patient Data Protection In National Legal Perspective,” Untag Law Rev., Vol. 8, No. 1, Pp. 28–40, 2024.

[14]M. Adhistya, J. S. Kekenusa, And J. S. V Sinolungan, “Socio-Technical Aspects Of Electronic Medical Record Use Related To Patient Safety At Prof Dr. Rd Kandou Manado Hospital,” Neo J. Econ. Soc. Humanit., Vol. 2, No. 2, Pp. 59–70, 2023.

[15]H. P. J. Wibowo, S. Suliyanto, And E. Sutrisna, “Evaluation Of The Implementation Of The Electronic Medical Record Information (Rme) System Based On User Perceptions Using The Technology Acceptance Model (Tam) Approach,” In Proceeding Of International Conference Sustainable Competitive Advantage, 2023, Vol. 4, No. 1.

[16]Z. N. Indira, A. P. Widodo, And F. Agushybana, “Literature Review: The Effectiveness Of Electronic Medical Records (Rme) On Hospital Service Quality,” J-Kesmas J. Fak. Kesehat. Masy. (The Indones. J. Public Heal., Vol. 10, No. 1, Pp. 57–64, 2023.

[17]E. W. Faida, P. F. Wiliyanarti, And M. M. D. Wahyuni, “Readiness Analysis Of Electronic Medical Record System (Rme): A Case Study Of Secondary Hospitals In Surabaya,” Heal. Technol. J., Vol. 1, No. 5, Pp. 461–473, 2023.

[18]E. P. Ginting, “Legal Analysis Of Patient Data Management Through Electronic Medical Records (Rme) In Anugerah Medical Laboratory: Desires And Reality,” In Proceedings: International Forum Research On Education, Social Sciences Technology And Humanities, 2024, Vol. 1, No. 2, Pp. 65–70.

[19]T. R. Akhmad, N. Pranadita, And S. Machmud, “Legal Protection Of Patients From Leakage Of Electronic Medical Records Data Is Reviewed From Law Number 27 Of 2022 Concerning Personal Data Protection And Law Number 17 Of 2023 Concerning Health,” Int. J. Asia Pasific Collab., Vol. 2, No. 3, 2024.