DINASTI RESEARCH
JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455

DOI: https://doi.org/10.38035/jlph.v5i2

Roles of Law on Medical Records for Data and Information Security: A Systematic Literature Review

Ida Bagus Udayana Hanggara[1], Tuty Kuswardhani[2], I Gusti Agung Gede Utara Hartawan[3].
[1]Magister Hukum Kesehatan, Universitas Udayana, Indonesia, oliputdyn@gmail.com.
[2]Magister Hukum Kesehatan, Universitas Udayana, Indonesia, tutykuswardhani@yahoo.com.
[3]Magister Hukum Kesehatan, Universitas Udayana, Indonesia, utara_hartawan@unud.ac.id.

Corresponding Author: oliputdyn@gmail.com[1]

Abstract: Electronic medical records must adhere to the principles of data and information security, which include availability, integrity, and confidentiality. Medical records serve as legitimate legal evidence, thereby satisfying these principles both individually and institutionally. Consequently, the aim of this research is to explore the roles of law on medical records for data and information security. To achieve this aim, a systematic literature review (SLR) was employed. The Scopus and PubMed databases were chosen for their global recognition. Full-text articles from these databases were subjected to PRISMA analysis using Mendeley Reference Manager. The researchers collected 32 research articles by the categories of data protection law, medical records' law enforcement, and data protection law recommendation. The research findings indicate that the roles of law deal with the role of law in compliance and data protection, law enforcement and sanctions, a recommendation for improving compliance and data protection. In addition, the law is crucial for ensuring compliance and data protection in electronic medical records implementation in hospitals. However, compliance levels have not reached optimal levels. To improve security, awareness, and enforcement, collaboration with legal bodies, and educational initiatives are needed. Legislation like HIPAA and GDPR influence data protection measures, but penalties are insufficient. To enhance compliance, medical personnel should undergo rigorous training and improve oversight of health data management procedures.

Keyword: Roles of Law, Medical Records, Medical Data, Information Security.

INTRODUCTION

The medical sector must meticulously balance the advancement of information technology with the preservation of stringent compliance standards and the safeguarding of personal data. In the current era of widespread technological progress linked to globalization, the electronic medical record system is a highly efficient and effective option for managing and storing patient health information (Sheikh et al., 2021). Regarding the deployment of electronic medical records in healthcare institutions, ensuring compliance and safeguarding data represent paramount concerns (Hussien et al., 2021). This is because the use of this system also gives rise to novel issues pertaining to the security of patient health information (Naarttijärvi, 2018). The swift advancement of digital technology in society is propelling the implementation of digitalization in health services. This necessitates electronic organization of medical records. This organization is required to comply with the principles of data security and protection, as well as the principles of safeguarding the information stored in the records. On August 31, 2022, the Ministry of Health issued Regulation Number 24 of 2022 regarding medical records. The purpose of this regulation was to supersede Regulation of the Minister of Health No. 269 of 2008, which previously governed medical records. The goal of this legislation was to address the community's needs in terms of both healthcare provisions and legal safeguards. Article 29 Paragraph (1) of Regulation of the Minister of Health Number 24 of 2022, officially known as Medical Records Regulation, mandates that electronic medical records must comply with data and information security standards (Evelyn Angelita Pinondang Manurung & Emmy Febriani Thalib, 2023).

The aforementioned principles encompass confidentiality, integrity, and availability. Acquiring comprehensive knowledge of the laws and regulations that control the use of electronic medical records in healthcare institutions is exceptionally crucial. It is critical to ensure that the use of technology for patient health data administration complies with the applicable legal regulations (Pratimaratri et al., 2019). Furthermore, this paper will also address the integration of technology in patient health data administration (Kusnadi, 2021). For the purpose of safeguarding patient health information, the technology employed must be capable of meeting rigorous data security and privacy criteria. Therefore, compliance is the paramount consideration for the implementation of electronic medical records in healthcare facilities (Meher et al., 2023). Strict adherence to the established rules is mandatory for all entities involved in the administration of patient health data, including medical staff and information technology professionals. Furthermore, ensuring data security should be a top priority (Susilayasa et al., 2024).

We must implement stringent protocols to guarantee the security of patient health information, averting inadvertent access by unauthorized individuals. In the current era, characterized by the relentless progress of information technology, the use of electronic medical records has become an indispensable necessity for the administration of patient health data and information. The electronic medical record system facilitates the storage, retrieval, and distribution of health insurance information with a notable degree of efficiency and reliability. However, to effectively implement this system, we must overcome certain obstacles. It is crucial to safeguard electronic medical records against unauthorized access, as they are considered legal documents (Budiyanti et al., 2019). Article 1, Number 6 of Law Number 19 of 2016, which changes Law Number 11 of 2008 on Information and Electronic Transactions (also known as the ITE Law), says that the people who use an electronic system, such as government officials, individuals, businesses, and/or citizens, are its organizers. In accordance with the ITE Law, the Electronic System is defined as the entity responsible for organizing the Electronic System.

Several regional general hospitals encounter diverse challenges concerning compliance and data security during the deployment of electronic medical records. One obstacle encountered is adherence to regulations regarding the privacy and security of protected patient data. Healthcare facilities are required to adhere to several privacy regulations and policies, including the Personal Data Protection Act and the Decree of the Minister of Health on Electronic Medical Record Standards, in order to preserve the confidentiality and integrity of patient data. Furthermore, it is imperative to implement efficient technical protocols to deter unauthorized entry into patient medical information, including the use of robust passwords, extensive system monitoring, and data encryption (Susilayasa et al., 2024). Furthermore, hospitals must confront obstacles in the integration of electronic medical record systems with other organizational information systems, including scheduling systems, financial systems, and pharmacy systems (Sagitariani et al., 2020). To ensure the entire system's efficiency and dependability, these functions must be capable of working synergistically and be well integrated.

In May 2021, the online media news source Republika.co.id published an article on the data breach handled by BPJS Kesehatan. BPJS Kesehatan members' unauthorized access to personal data contributes to a wide range of public data security concerns. Each individual's personal data contains crucial information that others can readily exploit for specific objectives, often causing harm to the respective owner (Nurpita, 2021). Implementing appropriate information technology in hospitals can enhance the effectiveness of the health service process, accelerate patient response times, and facilitate improved decision-making by medical staff (Elangovan et al., 2020). Furthermore, this system can also mitigate the likelihood of mistakes in the storage or retrieval of patient information, enhancing general patient safety (Abugabah et al., 2020). To achieve improved and safer healthcare services for patients receiving treatment at various regional public hospitals, hospitals must prioritize the optimization of compliance and data protection during the implementation of electronic medical records.

A former study conducted at Dr. Moewardi Hospital on the Legal Aspects of Electronic Medical Records revealed that each user is assigned a username and password to ensure privacy and confidentiality of data or information (Nugraheni & Nurhayati, 2018). Nevertheless, the use of this method is deemed suboptimal in ensuring data security in electronic medical records due to the susceptibility of the user's username and password to unauthorized acquisition by external entities. The requirement for data integrity in the Electronic Medical Record system, which means that data cannot be altered without permission from the authorized party, has not been effectively addressed (Nagasubramanian et al., 2020). Initially, the authentication component of the electronic medical record did not incorporate an electronic signature (Ganiga et al., 2020). The accessibility of information in the electronic medical record can be enhanced, but it is not yet at its maximum efficiency (Nugraheni & Nurhayati, 2018). The non-repudiation feature (anti-denial) of the electronic medical record has not been fully optimized in terms of identifying the party responsible for entering and modifying the corresponding information.

The study undertaken at Dharma Kerti Hospital, Tabanan, on the determination of hospital readiness in the implementation of electronic medical records is fully prepared for implementation (Maha Wirajaya & Dewi, 2020). Nevertheless, there are inherent limitations, specifically the lack of a dedicated team to expedite its execution. Deficiencies in Information Technology (IT), lack of a Standard Operating Procedure (SOP) pertaining to this matter, absence of a dedicated Electronic Medical Records team, absence of training on Electronic Medical Records, and absence of a designated budget or funds for the implementation of Electronic Medical Records (Maha Wirajaya & Dewi, 2020). We conducted a separate study to investigate medical personnel's adherence to digital medical data protection principles. The findings of the study revealed a notable and favorable correlation between the perceived usefulness and attitude towards data protection policies. An investigation by Pratimaratri et al. (2019) establishes a direct correlation between attitudes towards data protection and adherence to data protection regulations.

Practically, this study suggests that institutions must enhance attitudes towards data protection policies and perceived usefulness in order to bolster compliance behavior among medical staff. The present work makes a theoretical contribution to the technology acceptance paradigm. Compliance with digital medical data protection regulations is critical due to the data's personal and highly sensitive nature. The technology acceptance model posits that attitudes towards data protection serve as factors that influence behavioral intentions. Therefore, behavioral intentions serve as indicators of forthcoming behavior. In order to enhance data protection compliance, medical doctor institutions and hospital administration should focus on improving attitudes towards data protection. Enhancing behavioral intentions can also be achieved by optimizing attitudes towards data protection.

METHOD

This study utilized the systematic literature review (SLR) method to examine published works related to specific topics. The research primarily focused on instructional strategies in specific disciplines. The Scopus and the PubMed databases were chosen as a reference service due to their global recognition. The search process was organized into three categories: data protection law, medical records' law enforcement, and data protection law recommendation. Full-text articles from Scopus and PubMed databases were subjected to PRISMA analysis, including identification, screening, included, and meta-analysis feasibility using Mendeley Reference Manager. Relevant ideas were considered in the examination. The systematic planning process was applied to data protection law, medical records' law enforcement, and data protection law recommendation. Table 1 presents the results of systematic planning using Publish and Perish 8 on the Scopus and the PubMed databases between 2019 and 2024.

Table 1. The Systematic Planning using Publish and Perish 8 between 2019 and 2024

No	Category	PubMed	Scopus
1.	Data protection law	196	200
2.	Medical records' law enforcement	49	169
3.	data protection law recommendation	2	200
Total		247	569

The researchers conducted an analysis using the data presented above, which resulted in the collection of 247 papers from the PubMed database and 569 papers concerning the categories of data protection law, medical records' law enforcement, and data protection law recommendation. These papers were gathered in the Mendeley Reference Manager folder, exported as "RIS" data.

The systematic literature review (SLR) method employs five primary stages for the selection of literature: 1) The chosen publication data consists of full-text papers, excluding book reviews, theses, dissertations, book chapters, or proceedings, and only including research articles; 2) The selection of the full-text research articles is limited to those published within the last 5 years (2019-2024) and covers the categories determined by the researchers; 3) When conducting the investigation, the researchers exclusively rely on globally sourced data, specifically the Scopus and the PubMed databases as reputable journals with a strong reputation; 4) the researchers utilize specific applications such as Publish or Perish 8 and Mendeley reference management to facilitate the precise search for full text papers; 5) to obtain comprehensive global data on the three main themes mentioned above, researchers have opted to use the Scopus and the PubMed databases for their search for the full-text research articles.

RESULTS AND DISCUSSION

PRISMA Analysis Results

The process of searching for scientific publications was broken down into a number of different categories. These categories included data protection law, medical records' law enforcement, data protection law recommendation. Based on data connected to the inclusion and exclusion in literature selection, Figure 1 presents the article selection process based on the PRISMA systematic review flowchart.

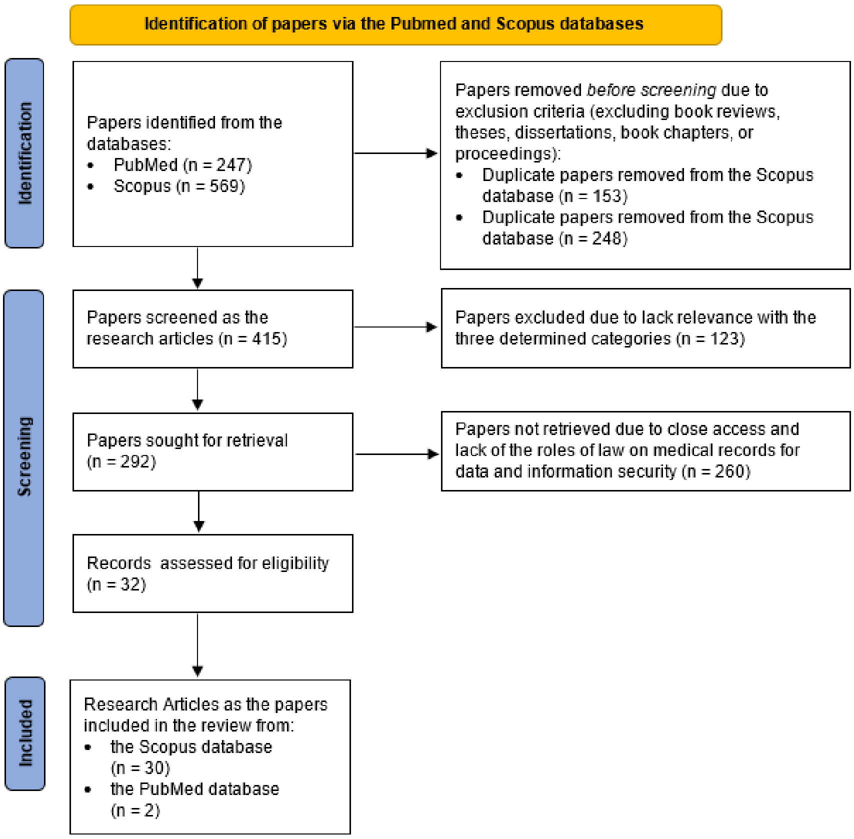
Identification of papers via the Pubmed and Scopus databases
Identification
Screening
Included
Papers identified from the databases:
• PubMed (n = 247)
• Scopus (n = 569)
Papers removed before screening due to exclusion criteria (excluding book reviews, theses, dissertations, book chapters, or proceedings):
• Duplicate papers removed from the Scopus database (n = 153)
• Duplicate papers removed from the Scopus database (n = 248)
Papers screened as the research articles (n = 415)
Papers excluded due to lack relevance with the three determined categories (n = 123)
Papers sought for retrieval (n = 292)
Papers not retrieved due to close access and lack of the roles of law on medical records for data and information security (n = 260)
Records assessed for eligibility (n = 32)
Research Articles as the papers included in the review from:
• the Scopus database (n = 30)
• the PubMed database (n = 2)

Figure 1. Article selection process based on the PRISMA systematic review flowchart

A comprehensive worldwide database, including Scopus and PubMed, was searched for publications published between 2019 and 2024. The search yielded 247 papers from the PubMed database and 569 from the Scopus database. However, 153 papers from the PubMed database and 248 from the Scopus database were removed due to exclusion criteria. After screening, 415 papers were left, with 123 articles excluded due to lack of relevance. 260 research articles were not retrieved due to close access and lack of understanding of the roles of law on medical records for data and information security. The researchers acquired 30 research articles with complete text of significant value from the Scopus database and 2 from the PubMed database. The RIS format was converted from Mendeley Reference Manager.

The Role of Law in Compliance and Data Protection

The law plays a crucial and irreplaceable role in ensuring compliance and safeguarding data during the implementation of electronic medical records in several general hospitals operating in the region. This is because the law acts as a robust basis for defining regulations and criteria concerning the handling of health data (Y. Chen et al., 2018; Murdoch, 2021). Moreover, this is the underlying cause for this situation. When considered within a wider framework, the function of law also assumes a significant role in guaranteeing that all processes pertaining to the gathering, retention, and use of health data are executed in a manner that is uniform with all relevant regulations (Argaw et al., 2020; Cheng et al., 2020; Price & Cohen, 2019). Furthermore, the legislation also serves another equally significant purpose, which is to protect the privacy rights of patients and to deter any improper use that may harm the individuals concerned (Kessler et al., 2019). Each of the parties concerned is vulnerable to experiencing negative consequences due to this situation, which has the capacity to escalate into a profound catastrophe.

From the study's findings, it can be inferred that the compliance and data protection levels in the implementation of electronic medical records in several general hospitals in the region have not yet achieved the expected optimal level. Moreover, the findings of this study indicate an urgent need to improve both the comprehension and consciousness of compliance standards, as well as the safeguarding of health data within the framework of health service organizations (Cilliers, 2019). Furthermore, the results of this study suggest that there exist deficiencies in the data security and protection system that require prompt resolution to avoid the potential misuse or breach of user health data by unauthorized entities (Mani et al., 2021). Timely and precise action must be taken to address this issue in order to guarantee the appropriate and optimal maintenance of user health data safety and protection.

In order to enhance awareness, skills, and understanding of the essentiality of adequately securing and safeguarding health data, it is imperative for relevant stakeholders to undertake deliberate and focused efforts. Furthermore, it is necessary to implement measures to enhance the use of technology that can strengthen and streamline the safeguarding of sensitive health data stored in the hospital's electronic medical record system (L. Chen et al., 2019). Effective enhancement of compliance and overall safeguarding of health data necessitates collaboration and mutual support among all stakeholders, including hospital administration, medical staff, and system users (Pirbhulal et al., 2019). The implementation of the electronic medical record system in several general hospitals in the region is expected to enhance the effectiveness, security, reliability, and trustworthiness of safeguarding the confidentiality and integrity of patients' health information (Srinivas et al., 2019). Furthermore, augmenting the use of state-of-the-art technology will not only contribute to the improvement of the quality and reliability of the electronic medical record system.

Moreover, to guarantee the preservation of user health information confidentiality, it is imperative for the different stakeholders to collaborate in a manner that is both cooperative and synergistic. The implementation of a more sophisticated data security and protection system will enable several general hospitals in the region to provide the utmost level of safeguarding for the health information of their patients (Lv & Qiao, 2020). By adopting this approach, the general population will experience a greater sense of comfort and are more inclined to place their trust in the hospital to avail themselves of the medical services it provides. Hence, it is imperative to enhance the criteria of adherence and safeguarding of health data, together with the implementation of more sophisticated technology, to ensure that electronic medical records in several general hospitals in the region attain the desired level of efficiency and dependability.

The Role of Law in Law Enforcement and Sanctions

In the context of health data compliance and protection, law enforcement and sanctions are crucial in upholding the integrity and security of health information in several general hospitals situated in the region. A number of regional general hospitals are responsible for enforcing health data management regulations, taking action against those violations (Wallace & Miola, 2021), and applying appropriate sanctions to anyone who violates relevant health data protection regulations (Shi et al., 2020; Thapa & Camtepe, 2021). The objective of this scenario is to provide a deterrent effect; hence, consistent law enforcement is of utmost importance (Vlahou et al., 2021). The objective is to guarantee that organizations intending to breach regulations pertaining to health data compliance and protection will carefully contemplate their actions before participating in activities that contravene the law.

By means of this deterrent effect, it is anticipated that the degree of consciousness regarding the need to adhere to legal regulations linked to health data can be far heightened. Given this, several general hospitals in the area will aggressively adopt and enhance the strategies that enable law enforcement to implement electronic medical records. Under this approach, regional general hospitals will implement proactive measures to ensure that any breach of health data compliance and protection is addressed decisively in accordance with the relevant legislation (Hathaliya & Tanwar, 2020). The maintenance of security and compliance is of paramount importance in the implementation of electronic medical records in several regional general hospitals (Vitunskaite et al., 2019). This goal can be achieved through effective cooperation with the appropriate legal authorities.

To enhance the enforcement of health data protection statutes, several regional general hospitals will collaborate closely with authorized legal and regulatory bodies (Azeez & der Vyver, 2019; da Veiga et al., 2020; Kaw et al., 2019). The implementation of this system will enable multiple regional general hospitals to not only prosecute any infractions internally (Kaplan, 2020; Keshta & Odeh, 2021), but also receive comprehensive backing from legal authorities to guarantee adherence to regulations and safeguard health data (Ahmad et al., 2021; Habibzadeh et al., 2019; Tanwar et al., 2020). The feasibility of this will be facilitated by the established collaboration among these hospitals will facilitate its feasibility (Li & Liu, 2021; Nifakos et al., 2021).

In order to enhance awareness of the importance of compliance and the safeguarding of health data, a number of regional general hospitals will actively execute educational initiatives targeting all members of the regional general hospitals and other relevant stakeholders. This will be undertaken with the purpose of increasing awareness. Enrolling in these programs will enable participants to develop a more profound understanding of the importance of maintaining the privacy of health information and the negative outcomes that arise from breaching relevant rules (Esmaeilzadeh, 2019; Sun et al., 2020). Several general hospitals in the area believe that providing thorough education will greatly improve awareness and adherence to health data regulations (Attaran, 2022; Hina & Dominic, 2020).

By addressing the medical information confidentiality concerns of the patients, the legitimacy of the information system, and the confidentiality of the registered entities, medical policies and ethics underscore the importance of law in safeguarding data and information safety in medical records. Legislation such as HIPAA in the United States and GDPR in the European Union significantly influences the criteria and regulations for protecting sensitive health information (Humphrey, 2021). These laws frequently include provisions that require providers, organizations, and other administrators of medical records to implement data protection measures, including encryption access controls and notification of breach procedures. However, these legislative provisions require informed consent and assurances regarding the use and protection of the data, given the unrestricted collection and retention of information. These legislative provisions dictate the minimum security requirements expected of affected organizations, such as health care providers. These requirements include preventing unauthorized access or release of electronic health records. These statutes outline the obligations that apply in the event of a security breach, which include notifying the public, authorities, and individuals (Ganiga et al., 2020). Additionally, legal mandates specify the organizational obligations of the health sector with respect to the safeguarding of data in the data-contained system. Adherence to these laws ensures the protection of individuals and organizations handling health information. However, the penalties imposed for breaking these laws only serve as a deterrent and do not stop vandalism.

Based on the findings of this research, these laws may undergo revisions as new technologies in human health care, such as telehealth services and other health care mobile applications, emerge. Consequently, it will be necessary to modify the data protection security protocols that are currently in place to address emerging vulnerabilities and risks. In addition to the international dimensions of health care and the movement of data across borders, it will be necessary to examine the extent to which data security regulations are in accordance with medical records. The debate centers on how regulatory frameworks impact privacy concerns ingrained in data security regulations, contrasting with the benefits of using data for research initiatives and public health promotion. Continuous amendment of laws is necessary to adequately protect and manage medical record data, given the dynamic nature of cyberspace threats.

This study proposes enhancing compliance and data protection in the deployment of electronic medical records in multiple regional general hospitals by adopting specific and thorough measures. The recommendation is based on the conclusive results of the research. In this specific situation, there are several methods by which one can achieve this goal. First and foremost, it is highly recommended that medical personnel and administrative officers directly involved in the field undergo rigorous and regular training periods (Evelyn Angelita Pinondang Manurung & Emmy Febriani Thalib, 2023; Kusnadi, 2021). Through engagement in this training, participants will acquire a more profound comprehension of the need to safeguard the privacy and integrity of data, as well as the methods by which sensitive data should not be treated inappropriately (Naarttijärvi, 2018). The training will provide participants with comprehensive instruction on compliance and data protection, empowering them to apply optimal methods in their daily professional practice.

Furthermore, we propose enhancing the oversight and assessment of health data management procedures in hospitals. This is a supplementary suggestion that we offer. The goal is to ensure that the existing procedures adhere to the necessary regulatory requirements for data security and privacy. A team of adept and seasoned experts in information security can undertake the task of supervision. These specialists have the capacity to carry out both regular evaluations and thorough inspections. Implementing this measure allows for the identification and efficient resolution of any deficiencies or vulnerabilities in the data management system after they have been detected. Furthermore, it is imperative to enhance the existing policies and controls aimed at safeguarding information security.

In order to ensure a safe and reliable environment for patients who use hospital services, several regional general hospitals must develop clear and resolute policies regarding the handling and safeguarding of electronic health information. To effectively implement this policy, it is necessary to include crucial elements, including the use of strong passwords, restricting access to sensitive information, and protecting data from cyber threats. In summary, it is imperative to establish rigorous information security measures to mitigate the risk of data breaches and the improper exploitation of health information. Data encryption is a prime illustration of the successful deployment of robust security measures.

Unauthorized access will be thwarted, and confidential information will be safeguarded from improperly authorized users. Moreover, it is imperative to enforce access limitations to guarantee that only persons with the requisite authority and need to consult health data are capable of doing so. In order to accomplish our goal of minimizing the probability of data breaches and improper utilization of health information, which can pose risks to patients and hospitals, we intend to implement these measures in several general hospitals in the region. Efficient and consistent implementation of these measures is critical to creating a safe and reliable environment for all individuals who use the services provided by several general hospitals in the area.

CONCLUSION

The law plays a crucial role in ensuring compliance and data protection during the implementation of electronic medical records in various general hospitals in the region. It acts as a robust basis for defining regulations and criteria concerning the handling of health data, protecting patient privacy rights, and deterring improper use that may harm individuals. However, the compliance and data protection levels in the implementation of electronic medical records have not yet reached the expected optimal level. The study indicates an urgent need to improve understanding and consciousness of compliance standards and safeguarding health data within health service organizations. There are deficiencies in the data security and protection system that require prompt resolution to avoid potential misuse or breach of user health data by unauthorized entities. To ensure the appropriate and optimal maintenance of user health data safety and protection, it is imperative to enhance awareness, skills, and understanding of the importance of adequately securing and safeguarding health data.

In the context of health data compliance and protection, law enforcement and sanctions are crucial in upholding the integrity and security of health information in several general hospitals situated in the region. Regional general hospitals are responsible for enforcing health data management regulations, taking action against violations, and applying appropriate sanctions to those who violate relevant health data protection regulations. To enhance the enforcement of health data protection statutes, regional general hospitals will collaborate closely with authorized legal and regulatory bodies. Educational initiatives targeting all members of the hospital and other relevant stakeholders will be undertaken to increase awareness of the importance of compliance and the negative outcomes that arise from breaching relevant rules.

Medical policies and ethics emphasize the importance of law in safeguarding data and information safety in medical records. Legislation such as HIPAA in the US and GDPR in the European Union significantly influence the criteria and regulations for protecting sensitive health information. These laws require providers, organizations, and administrators of medical records to implement data protection measures, including encryption access controls and notification of breach procedures. However, these laws require informed consent and assurances regarding the use and protection of the data. Adherence to these laws ensures the protection of individuals and organizations handling health information. However, penalties imposed for breaking these laws only serve as a deterrent and do not stop vandalism. As new technologies in human health care emerge, it will be necessary to modify data protection security protocols to address emerging vulnerabilities and risks.

This study proposes enhancing compliance and data protection in the deployment of electronic medical records in multiple regional general hospitals by adopting specific and thorough measures. Medical personnel and administrative officers should undergo rigorous training periods to understand the importance of safeguarding privacy and integrity of data. Additionally, enhancing oversight and assessment of health data management procedures in hospitals is crucial to ensure the necessary regulatory requirements for data security and privacy.

REFERENCE

Abugabah, A., Nizamuddin, N., & Abuqabbeh, A. (2020). A review of challenges and barriers implementing RFID technology in the Healthcare sector. Procedia Computer Science, 170, 1003–1010. https://doi.org/https://doi.org/10.1016/j.procs.2020.03.094

Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. International Journal of Medical Informatics, 148, 104399. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2021.104399

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1), 70–83. https://doi.org/10.1080/20479700.2020.1843887

Azeez, N. A., & der Vyver, C. Van. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), 97–108. https://doi.org/https://doi.org/10.1016/j.eij.2018.12.001

Budiyanti, R., Herlambang, P., & Nandini, N. (2019). Tantangan etika dan hukum penggunaan rekam medis elektronik dalam era personalized medicine. Jurnal Kesehatan Vokasional, 4, 49. https://doi.org/10.22146/jkesvo.41994

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems, 95, 420–429. https://doi.org/https://doi.org/10.1016/j.future.2019.01.018

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems, 43(1), 5. https://doi.org/10.1007/s10916-018-1121-4

Cheng, X., Chen, F., Xie, D., Sun, H., & Huang, C. (2020). Design of a Secure Medical Data Sharing Scheme Based on Blockchain. Journal of Medical Systems, 44(2), 52. https://doi.org/10.1007/s10916-019-1468-1

Cilliers, L. (2019). Wearable devices in healthcare: Privacy and information security issues. Health Information Management Journal, 49(2–3), 150–156. https://doi.org/10.1177/1833358319851684

da Veiga, A., Astakhova, L. V, Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/https://doi.org/10.1016/j.cose.2020.101713

Elangovan, D., Long, C. S., Bakrin, F. S., Tan, C. S., Goh, K. W., Hussain, Z., Al-Worafi, Y. M., Lee, K. S., Kassab, Y. W., & Ming, L. C. (2020). Application of Blockchain Technology in Hospital Information System. In Mathematical Modeling and Soft Computing in Epidemiology (1st Editio, p. 16). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003038399-12/application-blockchain-technology-hospital-information-system-deepa-elangovan-chiau-soon-long-faizah-safina-bakrin-ching-siang-tan-khang-wen-goh-zahid-hussain-yaser-mohammed-al-worafi-kah-seng-lee-yaman-walid-kassab-long-chiau-ming

Esmaeilzadeh, P. (2019). The Effects of Public Concern for Information Privacy on the Adoption of Health Information Exchanges (HIEs) by Healthcare Entities. Health Communication, 34(10), 1202–1211. https://doi.org/10.1080/10410236.2018.1471336

Evelyn Angelita Pinondang Manurung, & Emmy Febriani Thalib. (2023). Tinjauan yuridis perlindungan data pribadi berdasarkan UU nomor 27 tahun 2022. Jurnal Hukum Saraswati, 4(2 SE-), 139–148. https://e-journal.unmas.ac.id/index.php/JHS/article/view/5941

Ganiga, R., Pai, R. M., Pai, M. M., & Sinha, R. K. (2020). Security framework for cloud based electronic health record (EHR) system. International Journal of Electrical and Computer Engineering, 10, 455–466.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660. https://doi.org/https://doi.org/10.1016/j.scs.2019.101660

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153, 311–335. https://doi.org/https://doi.org/10.1016/j.comcom.2020.02.018

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems, 60(3), 201–211. https://doi.org/10.1080/08874417.2018.1432996

Humphrey, B. A. (2021). Data Privacy vs. Innovation: A Quantitative Analysis of Artificial Intelligence in Healthcare and Its Impact on HIPAA regarding the Privacy and Security of Protected Health Information [Robert Morris University]. https://doi.org/28549541

Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H., & Salman, S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration, 22, 100217. https://doi.org/https://doi.org/10.1016/j.jii.2021.100217

Kaplan, B. (2020). Revisiting health information technology ethical, legal, and social issues and evaluation: Telehealth/telemedicine and COVID-19. International Journal of Medical Informatics, 143, 104239. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2020.104239

Kaw, J. A., Loan, N. A., Parah, S. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2019). A reversible and secure patient information hiding system for IoT driven e-health. International Journal of Information Management, 45, 262–275. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.09.008

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. https://doi.org/https://doi.org/10.1016/j.eij.2020.07.003

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2019). Information security climate and the assessment of information security risk among healthcare employees. Health Informatics Journal, 26(1), 461–473. https://doi.org/10.1177/1460458219832048

Kusnadi, S. (2021). Perlindungan hukum data pribadi sebagai hak privasi. AL WASATH Jurnal Ilmu Hukum, 2, 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/https://doi.org/10.1016/j.egyr.2021.08.126

Lv, Z., & Qiao, L. (2020). Analysis of healthcare big data. Future Generation Computer Systems, 109, 103–110. https://doi.org/https://doi.org/10.1016/j.future.2020.03.039

Maha Wirajaya, M., & Dewi, N. M. U. (2020). Analisis kesiapan Rumah Sakit Dharma Kerti Tabanan menerapkan rekam medis elektronik. Jurnal Kesehatan Vokasional, 5, 1. https://doi.org/10.22146/jkesvo.53017

Mani, V., Manickam, P., Alotaibi, Y., Alghamdi, S., & Khalaf, O. I. (2021). Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. In Electronics (Vol. 10, Issue 23). https://doi.org/10.3390/electronics10233003

Meher, C., Sidi, R., & Risdawati, I. (2023). Penggunaan data kesehatan pribadi dalam Era Big Data: Tantangan hukum dan kebijakan di Indonesia. Jurnal Ners, 7, 864–870. https://doi.org/10.31004/jn.v7i2.16088

Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Medical Ethics, 22(1). https://doi.org/10.1186/s12910-021-00687-3

Naarttijärvi, M. (2018). Balancing data protection and privacy – The case of information security sensor systems. Computer Law & Security Review, 34(5), 1019–1038. https://doi.org/https://doi.org/10.1016/j.clsr.2018.04.006

Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi4, A. H., Balusamy, Sankayya, M., & Balamurugan. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing & Applications, 32(3), 639–647. https://doi.org/10.1007/s00521-018-3915-1

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare

Organisations: A Systematic Review. In Sensors (Vol. 21, Issue 15). https://doi.org/10.3390/s21155119

Nugraheni, S. W., & Nurhayati. (2018). Aspek hukum rekam medis elektronik di RSUD Dr. Moewardi. Prosiding Seminar Nasional Unimus Volume 1, 97.

Nurpita, S. (2021). Data pribadi BPJS Kesehatan bocor, masyarakat dirugikan. Republika. https://sindikasi.republika.co.id/ berita/qtthfk282 /data-pribadi-bpjs-kesehatan-bocor-masyarakat- dirugikan

Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. Future Generation Computer Systems, 95, 382–391. https://doi.org/https://doi.org/10.1016/j.future.2019.01.008

Pratimaratri, U., Ilona, D., & Zaitul, Z. (2019). Digital medical data protection compliance among medical staffs. Journal of Physics Conference Series, 1339, 1–7. https://doi.org/10.1088/1742-6596/1339/1/012100

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. Nature Medicine, 25(1), 37–43. https://doi.org/10.1038/s41591-018-0272-7

Sagitariani, S., Januraga, P. P., & Negara, I. (2020). Delphi approach to explore ways to optimize case manager services in inpatient wards of Sanglah General Hospital. Public Health and Preventive Medicine Archive, 8, 150. https://doi.org/10.15562/phpma.v8i2.310

Sheikh, A., Anderson, M., Albala, S., Casadei, B., Franklin, B. D., Richards, M., Taylor, D., Tibble, H., & Mossialos, E. (2021). Health information technology and digital innovation for national learning health and care systems. The Lancet Digital Health, 3(6), e383–e396. https://doi.org/10.1016/S2589-7500(21)00005-4

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97, 101966. https://doi.org/https://doi.org/10.1016/j.cose.2020.101966

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178–188. https://doi.org/https://doi.org/10.1016/j.future.2018.09.063

Sun, Z., Strang, K. D., & Pambel, F. (2020). Privacy and security in the big data paradigm. Journal of Computer Information Systems, 60(2), 146–155. https://doi.org/10.1080/08874417.2017.1418631

Susilayasa, I. K. A., Susanti, N. L. P. D., Wahyuningsih, L. G. N. S., & Wulandari, I. A. P. (2024). Case manager experience in health services in regional hospitals in Bali. Indonesian Journal of Global Health Research, 6(4 SE-Articles). https://doi.org/10.37287/ijghr.v6i4.3219

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. https://doi.org/https://doi.org/10.1016/j.jisa.2019.102407

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in Biology and Medicine, 129, 104130. https://doi.org/https://doi.org/10.1016/j.compbiomed.2020.104130

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. Computers & Security, 83, 313–331. https://doi.org/https://doi.org/10.1016/j.cose.2019.02.009

Vlahou, A., Hallinan, D., Apweiler, R., Argiles, A., Beige, J., Benigni, A., Bischoff, R., Black, P. C., Boehm, F., Céraline, J., Chrousos, G. P., Delles, C., Evenepoel, P., Fridolin, I., Glorieux, G., van Gool, A. J., Heidegger, I., Ioannidis, J. P. A., Jankowski, J., … Vanholder, R. (2021). Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics? Hypertension (Dallas, Tex. : 1979), 77(4), 1029–1035. https://doi.org/10.1161/HYPERTENSIONAHA.120.16340

Wallace, S. E., & Miola, J. (2021). Adding dynamic consent to a longitudinal cohort study: A qualitative study of EXCEED participant perspectives. BMC Medical Ethics, 22(1), 12. https://doi.org/10.1186/s12910-021-00583-w.