Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan
Vol. 11, No. 1, June 2025
http://ejournal.undip.ac.id/index.php/lpustaka

Research Article
Received: 22 January 2025, Revised: 15 April 2025, Accepted: 6 May 2025, Online: 1 June 2025

Focused Analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data Security Implementation of Electronic Medical Records at Sindangwangi Health Center, Pangandaran, West Java

Fina Julia[1)*], Dwi Ridho Aulianto[2)]
[1)]*D4 Archival Study Program, Indonesia Open University, Indonesia*
[2)]*National Research and Innovation Agency, Jakarta, Indonesia*
[1)*]finaajuliaa1707@gmail.com, [2)]dwir007@brin.go.id

Abstract

Background: Digital transformation in the healthcare sector requires the management of medical records to be conducted electronically, with emphasis on the principles of data security, including confidentiality, integrity, and availability.

Objective: This research aims to analyze the management of electronic medical record data security at the Sindangwangi Health Center in accordance with Article 29 of the Indonesian Minister of Health Regulation Number 24 of 2022.

Methods: This study employs a descriptive qualitative method, collecting data through interviews and observations with informants, including one medical record officer and one registration officer, conducted from October to November 2024.

Results: The management of EMR data security at Puskesmas Sindangwangi demonstrates a solid application of the CIA principles. Confidentiality is maintained through unique usernames and passwords that are updated every three months and an automatic log-out feature after inactivity. Integrity is upheld by restricting data editing to authorized personnel, with changes allowed only after one month. Availability is supported by a cloud-based system that enables real-time access. However, challenges remain, including incomplete data entry in the Emergency Department, technical disruptions such as server downtime and power outages, the use of manual systems in the cashier unit, and the absence of formal vendor agreements and disaster recovery planning.

Conclusion: While the EMR system shows effective initial implementation of data security principles, improvements are needed in infrastructure, staff training, system integration, and vendor governance to ensure a more resilient and secure digital health system.

Keywords: Data Security, Puskesmas Sindangwangi, EMR, Confidentiality, Integrity, Availability

INTRODUCTION

Digital transformation in healthcare services, driven by advances in information technology, necessitates that medical record management be conducted electronically, with attention to the principles of security, confidentiality, integrity, and data availability. The Indonesian Minister of Health Regulation Number 24 of 2022 concerning Medical Records was introduced because the previous regulation, Minister of Health Regulation Number 269/MENKES/PER/III/2008, is no longer relevant to current developments in science and

[*] Corresponding Author

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

technology. Therefore, a new regulation that aligns more closely with the dynamics of technology and the needs of modern healthcare services is required. Through the Indonesian Minister of Health Regulation Number 24 of 2022, the government mandates that every community health center and other healthcare services manage patient data digitally using an Electronic Medical Record system (Yunisca et al., 2022).

In developed countries, Electronic Medical Records (EMR) are widely used to manage information related to patient treatment records. EMR is a digital system that stores patient health information, from medical history to treatments administered (Ismatullah et al., 2023). The use of EMR offers various benefits, including facilitating consultations between doctors and patients, as well as simplifying access to and management of health data (Keshta & Odeh, 2021). The implementation of EMR is expected to create comprehensive medical record keeping to support various aspects of healthcare services, from patient management to the generation of reports and relevant data analysis. Furthermore, EMR is anticipated to enhance communication, making information access easier for healthcare providers and speeding up the process of accurate reporting on patient services. EMR is also utilized for various other purposes, such as quality service management, reporting service outcomes, resource planning, and public health management (Indradi, 2020). Medical records are crucial in health center services, and their management must be performed optimally in accordance with applicable regulations. This is an important step to ensure the quality of healthcare services provided (Nisa et al., 2024). EMR greatly assists and simplifies the work of medical record keepers, particularly in recording patient data, registering new patients, and retrieving necessary information (Tasbihah & Yunengsih, 2024).

With the advancement of technology, the management of sensitive and personal patient data has become increasingly complex. Therefore, the protection of patient data security and confidentiality in the implementation of health technologies has become crucial (Suci et al., 2018). Data security processes are designed to protect the confidentiality, integrity, and availability of data (Pratiwi et al., 2022). Patient data confidentiality must be safeguarded by equipping electronic medical record systems with various security mechanisms, such as data encryption, stringent access controls, and network protection against cyberattacks. Given that patient medical records are sensitive personal data, special protection is essential. Information such as identity, examination results, and treatment records must be secured to prevent unauthorized access (Joel et al., 2023).

The success of implementing Electronic Medical Records (EMR) relies on the quality of human resources. Improving the competency of healthcare personnel in using EMR is essential, necessitating training for all users (Izza & Lailiyah, 2024). A stable internet connection is also crucial, as it affects EMR performance, including access speed and real-time data updates. Connectivity issues like power outages can disrupt data entry and risk data loss (Amin et al., 2021). Errors in EMR usage can lead to serious problems, so various factors such as data types and formats must be considered in system development (Zulkipli et al., 2022). Identifying privacy and security issues in healthcare institutions and evaluating solutions is vital for protecting patient confidentiality. IT security in healthcare systems must also be monitored (Keshta & Odeh, 2021).Standard Operating Procedures (SOPs) serve as important guidelines

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

for the implementation of EMRs in community health centers and other healthcare services. SOPs provide clear working instructions for healthcare personnel when recording medical records, thereby minimizing errors and ensuring the quality of the recorded data. With SOPs in place, the medical record documentation process becomes more structured and efficient (Izza & Lailiyah, 2024). One of the primary objectives of having SOPs in work units is to reduce the likelihood of errors in task execution. In Electronic Medical Records, SOPs play a critical role in preventing data recording mistakes that could disrupt the system (Taufiq, 2019).

According to the Regulation of the Minister of Health of the Republic of Indonesia Number 43 of 2019 concerning Community Health Centers (Puskesmas), Puskesmas is a primary health service unit responsible for providing public health services. The main focus of Puskesmas is on promotive and preventive aspects, aimed at optimally improving the health quality of the community in its working area. In line with this goal, Puskesmas Sindangwangi has the vision of "Creating a Self-Reliant Community in the Working Area of Puskesmas Sindangwangi for Healthy Living by 2024." The mission of Puskesmas Sindangwangi includes: improving quality health services, ensuring equitable and adequate health resources, empowering the community to adopt healthy lifestyles, and developing mutually beneficial partnerships.

Puskesmas Sindangwangi has issued a Policy Letter (SK) related to the Implementation of Electronic Medical Records and SK regarding Access to Medical Records. Based on the Decree of the Head of the Regional Technical Implementation Unit (UPTD) of Puskesmas Sindangwangi Number 445.4/263-SK/PKMSDW/IV/2023 concerning the Implementation of Medical Records, it is important to establish standards and classifications of diagnoses as well as terminology used to support disease diagnoses and improve the quality of clinical services. Furthermore, the Decree of the Head of UPTD Puskesmas Sindangwangi Number 445.4/264-SK/PKMADW/IV/2023 regarding Access to Medical Records outlines the importance of adhering to data and information security principles, which include confidentiality, integrity, and availability of medical records. Therefore, it is necessary to establish access rights to medical records to ensure the security of that information.

Several studies on the security and confidentiality of electronic medical records have been conducted. Among them is the study by We'e, Nugroho, and Siswatibudi (2023) titled "Evaluation of Security and Confidentiality Aspects of Electronic Medical Records at Panti Nugroho Hospital." This study indicates that the implementation of confidentiality and security aspects of electronic medical records (RME) has been running well. To maintain the confidentiality of patient data, the system applies unique user IDs and passwords for each healthcare worker and restricts access rights according to their authority. However, technical obstacles, such as system disturbances and unstable internet connections, still frequently occur. Therefore, there is a need to enhance the infrastructure to optimally support the system's performance. Furthermore, a study by Ardianto and Nurjanah (2024) titled "Analysis of Patient Data Security Aspects in the Implementation of Electronic Medical Records at Hospital X" reveals that the security of the RME system at Hospital X already uses username and password-based authentication, as well as electronic signatures. Nevertheless, the system still faces several challenges, such as the absence of standard operating procedures (SOP) for periodic

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

password changes, which can increase the risk of unauthorized access. Additionally, the system limits flexibility in editing data, especially for large volumes of data. Despite this, the system has implemented access restrictions and tracking mechanisms to maintain data integrity.

Based on the background described, this research aims to analyze the management of electronic medical record data security in accordance with the Indonesian Minister of Health Regulation No. 24 of 2022 Article 29 at Puskesmas Sindangwangi. This study is expected to contribute to understanding the challenges and solutions necessary to improve the security of electronic medical record data, enabling more effective and secure healthcare services at Puskesmas Sindangwangi.

LITERATURE REVIEW

The security of electronic medical record (EMR) data is paramount at the Sindangwangi Health Center in Pangandaran, West Java, particularly under the implementation of Regulation Number 24 of 2022 by the Indonesian Minister of Health. This regulation mandates the systematic adoption of EMRs across healthcare facilities, aiming to integrate patient data for improved health mapping while ensuring data confidentiality and security (Larasati et al., 2024; Mahendika & Setyowati, 2023).

However, the implementation of this regulation faces significant challenges. Limited internet access and inadequate preparedness among healthcare practitioners hinder effective adoption (Larasati et al., 2024). The regulation imposes administrative consequences for non-compliance, such as potential revocation of accreditation, highlighting the critical need for adherence to security standards (Mahendika & Setyowati, 2023).

Moreover, infrastructural shortcomings, particularly in remote areas, exacerbate the difficulties in securely handling medical records (Putri & Mulyanti, 2023; Pujiarno, 2024). The Personal Data Protection Act complements these efforts by providing a legal framework for safeguarding personal health data; however, gaps in enforcement and public awareness remain prevalent ("Protection of Medical Record Data as a Form of Legal Protection of Health Data through the Personal Data Protection Act," 2023; Prayuti, 2024; Judijanto et al., 2024).

To mitigate risks of unauthorized access and data breaches, security measures such as encryption, individual authentication, and regular audits are recommended (Pradita et al., 2022; PB & Sutabri, 2024). The Sindangwangi Health Center, like other facilities, must enhance its information security management systems and ensure compliance with both national regulations and best practices in data protection to effectively safeguard patient privacy (Katsikas, 2013; Putrawansyah & Sutabri, 2024).

In conclusion, while the regulatory framework establishes a robust foundation for EMR security, its successful implementation hinges on addressing infrastructural challenges and raising public awareness, alongside rigorous enforcement of security protocols (Larasati et al., 2024; Putri & Mulyanti, 2023; Prayuti, 2024).

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

METHODS

This research is qualitative, using descriptive data from written text and conversations to explore the deeper meanings of observed phenomena. The qualitative method is grounded in postpositivism, meaning the research occurs in the natural setting of the subjects, with the researcher as a key instrument. The focus is on qualitative data analysis rather than generating generalizations applicable to all cases; it emphasizes a deep understanding of meanings within specific social contexts (Muljono et al., 2022).

The study is conducted at the Medical Records Unit of Puskesmas Sindangwangi, located at Jalan Raya Pangandaran No. 753, Padaherang District, Pangandaran Regency, West Java. Data collection occurred from October to November 2024, using interviews and observations. Informants included one medical records officer and one registration officer. Interviews aimed to assess the management and implementation of Electronic Medical Record (EMR) data security in accordance with regulations and identify obstacles related to confidentiality, integrity, and availability of data. Interviews are a popular method in qualitative research for obtaining primary data in interpretive and critical studies (Hartono, 2018). Observations were conducted to understand the management and implementation of EMR data security at Puskesmas Sindangwangi, encompassing complex phenomena involving interrelated biological and psychological processes (Sugiyono, 2016).

To ensure data validity, this study employed methodological triangulation by comparing data obtained from interviews with those gathered through field observations. In addition, member checking was conducted by confirming the interview results with the informants to ensure the accuracy of the data and the researcher’s interpretation. These steps are essential to minimize bias and strengthen the credibility of the research findings.

This study has a primary limitation regarding the number of informants, which consisted of only two individuals: the medical records officer and the registration officer. This limitation may affect the completeness and diversity of perspectives obtained. However, this condition is inseparable from the organizational structure and the limited human resources available at Sindangwangi Health Center, particularly in the management of electronic medical records (EMR). Therefore, the findings of this study emphasize an in-depth understanding of the local context and are not intended to be generalized to other health centers with different conditions.

Data analysis occurred post-collection (Hartono, 2018), continuously from data gathering to completion. Analyzed data included interview and observation results, with systematic steps involving data reduction, presentation, and conclusion drawing as outlined in qualitative data processing (Miles, Huberman & Saldaña, 2014).

FINDINGS AND DISCUSSION

The implementation of Electronic Medical Records (EMR) at Puskesmas Sindangwangi reflects a growing commitment to digital health transformation. Data security

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

within the EMR system is managed through the application of the CIA principles: Confidentiality, Integrity, and Availability. Although several mechanisms have been established to support these principles, there remain significant gaps between policy and practice that require attention.

Confidentiality: Access Controls and Vendor Dependency

Confidentiality is primarily maintained through user authentication and role-based access control (RBAC). Each staff member is assigned a unique username and password, which must be updated every three months to reduce password fatigue and prevent unauthorized access. Access rights are determined by job functions—for example, nurses may only input or view anamnesis data, pharmacy staff access only medication records, and administrative staff are restricted to registration modules.

The system also includes automatic logout after 10–15 minutes of inactivity, serving as a safeguard against unauthorized access in shared or unattended workstations. However, a critical gap in this framework is the reliance on third-party vendors for data recovery and backup. Although vendors are tasked with restoring data during system failures or losses, there is no documented Standard Operating Procedure (SOP) or formal contractual agreement outlining the vendor’s responsibilities, response times, or data protection standards. This overreliance without defined accountability creates potential vulnerabilities, especially during emergencies or vendor transitions.

Integrity: Controlled Editing but Lack of Transparency

To uphold data integrity, the system restricts editing capabilities to authorized personnel. Patient data can only be modified after a one-month waiting period following the visit. This policy is intended to avoid unintentional or unauthorized modifications and encourage careful review before making any corrections.

The EMR system captures comprehensive personal and administrative patient data, including unique identifiers such as the patient’s eRM number, national ID, and complete address details. While the editing restriction is a strength, the lack of audit trails, data encryption, or periodic integrity checks presents a major weakness. Without an audit log, it is difficult to trace who made changes, when, and under what context, making accountability and data tracking problematic.

Availability: Broad Access with Infrastructural Challenges

The EMR system is accessible via a cloud-based platform that enables staff to retrieve and input patient data from any device with an internet connection. This flexibility supports real-time access and continuity of care. Currently, all clinical units have adopted EMR use—with the exception of the cashier unit, which continues to rely on manual systems. This lack of integration creates inefficiencies in billing and administrative workflows, reducing the effectiveness of centralized health information management.

Despite broad accessibility, infrastructure limitations persist, especially in the form of power outages and internet disruptions. During such events, staff revert to manual documentation, which is later transcribed into the EMR. While this approach provides a short-term workaround, it increases the risk of data inconsistencies and delays. Moreover, there is no comprehensive disaster recovery plan in place beyond vendor intervention, indicating a low level of system resiliency in the face of prolonged downtime.

Human Resource and Policy Implementation Issues

The rollout of the EMR system began in 2023, with medical record officers and physicians adequately trained in its operation. However, disparities in digital literacy, particularly among older staff and those in high-pressure units such as the Emergency Room (ER), remain a challenge. Training is ongoing, but current methods may be too rapid or technical for all employees to fully comprehend. Adjustments in training delivery—such as slower-paced, hands-on sessions—are needed to bridge this gap.

In addition, some staff have experienced difficulties with data entry and attendance reporting, especially in time-sensitive clinical settings. Technical support is provided by the internal IT team or, when escalated, through vendor assistance. However, the absence of a clear incident response plan or tiered escalation process often leads to delays in resolving critical system issues.

TABLE 1
IMPLEMENTATION OF CIA PRINCIPLES IN EMR AT PUSKESMAS SINDANGWANGI

Principle	**Regulatory Standard (Permenkes 24/2022, Article 29)**	**Implementation at Puskesmas Sindangwangi**	**Gaps/Notes**
Confidentiality	Access only by authorized personnel; protection from unauthorized access	Username/password for each staff; role-based access; vendor manages recovery	Lack of documented SOP/vendor contract; over-reliance on vendor
Integrity	Data accuracy, completeness, and accountability	Editing allowed by authorized personnel; corrections after 1 month	No audit trail or encryption details reported
Availability	Data must be available when needed	Web-based/cloud access; accessible via mobile; all units except cashier	Cashier unit not yet integrated; network/power disruptions

DISCUSSION

Overall, the EMR system at Puskesmas Sindangwangi reflects a foundational yet evolving understanding of data security principles. The institution has taken positive initial steps, such as implementing unique user credentials, enforcing password update cycles, and applying role-based access restrictions. These features align with basic best practices in digital health information management. However, critical components—particularly in the areas of

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

vendor management, system resilience, and audit transparency—remain underdeveloped and pose significant risks to data security and organizational accountability.

One major concern is the absence of formal agreements with third-party vendors, who currently manage data recovery operations. While outsourcing to external providers offers specialized expertise and can be cost-effective, it also introduces serious vulnerabilities. Without written contracts, service-level agreements (SLAs), or defined escalation procedures, Puskesmas Sindangwangi risks facing service delays, uncoordinated responses during emergencies, and exposure to privacy breaches. This is especially relevant in light of increasing data breach incidents linked to third-party access in healthcare settings (VanHoy, 2021). Therefore, developing robust vendor governance—anchored in clear documentation and regular performance reviews—is imperative for strengthening institutional control over external operations.

From an operational standpoint, the EMR system has been adopted across most clinical units, yet full integration is still lacking. Notably, the cashier unit continues to rely on manual systems, creating disconnects in service delivery and data consolidation. Full digital integration is crucial not only for administrative efficiency but also for enhancing transparency in billing and financial tracking. Moreover, successful EMR adoption hinges on human resource capacity. As emphasized by Denkovski et al. (2024), many cybersecurity vulnerabilities are rooted in low user awareness and inconsistent digital competencies. Investing in regular, targeted staff training—particularly for older employees or those in high-pressure environments like emergency care—can significantly reduce operational risks.

Although access to the EMR is secured by authentication mechanisms and usage policies, the absence of audit trails, data encryption, and routine data integrity checks poses a significant threat to both data accuracy and regulatory compliance. The current system does not track who accessed or edited data, which weakens accountability and hampers incident investigation. Integrating features such as AES-based encryption and One-Time Passwords (OTP), as recommended by Ononiwu & MgBeafulike (2024), would create a more secure and verifiable data environment. Furthermore, checksum-based verification methods and integrity audits could ensure that data remains consistent and tamper-free over time.

Nonetheless, strengthening data security must be done in tandem with maintaining system interoperability and usability. One of the long-standing challenges in EMR implementation is balancing robust security with the need for efficient information exchange. As Shrivastava et al. (2019) point out, overly restrictive access controls may hinder the flow of clinical information across departments or with referral hospitals, undermining patient care continuity. Puskesmas Sindangwangi should consider adopting interoperable standards such as HL7 or FHIR while reinforcing layered access permissions to protect data without impeding clinical workflows.

To address these challenges holistically, a multidisciplinary cybersecurity strategy is required. This strategy should incorporate technical defenses (e.g., firewall systems, intrusion detection), organizational procedures (e.g., SOPs, regular audits), and legal compliance (e.g., alignment with national health IT laws and data protection regulations). As suggested by Cellier & Ghernaouti (2019), integrating all three dimensions creates a resilient framework capable of withstanding the evolving threat landscape. In addition, Puskesmas Sindangwangi should implement routine internal audits, risk assessments, and anomaly detection systems to proactively identify and mitigate security issues.

Equally vital is the cultivation of a strong security culture within the organization. A culture of security moves beyond formal training and requires active engagement, open dialogue about risks, and leadership by example. Staff at all levels should feel responsible for protecting patient data, and managers must reinforce this responsibility through visible commitment and ongoing communication. Sharing lessons learned from prior incidents and involving end-users in policy development are proven ways to foster ownership and increase policy adherence.

This discussion does not only assess internal performance at Puskesmas Sindangwangi but also contextualizes it within the broader discourse on healthcare information security. The institution’s experience parallels the challenges documented in global literature and highlights the common need for better documentation, increased staff competency, and stronger technical infrastructure. By benchmarking its progress against these external insights, Puskesmas Sindangwangi is better positioned to identify strategic improvement areas and anticipate future risks.

Despite progress, this study acknowledges several key limitations. A prominent one is the lack of objective evaluations of vendor performance. No structured metrics or feedback mechanisms currently exist to monitor vendor compliance with expected standards. Additionally, while the EMR is operational in most units, the lack of full integration with financial and administrative functions (such as the cashier) represents a significant bottleneck in achieving holistic data management. These operational gaps are compounded by disparities in digital adaptability among staff, particularly older employees or those unfamiliar with cloud-based platforms.

In summary, Puskesmas Sindangwangi has made commendable strides in implementing Electronic Medical Records as part of its broader digital transformation agenda. However, the long-term security, resilience, and usability of the system require continuous refinement. A three-pronged approach is recommended: (1) strengthening technical safeguards—such as encryption, audit trails, and multifactor authentication; (2) formalizing vendor partnerships with clear contracts and performance benchmarks; and (3) investing in human capital through continuous training and cultural change initiatives. Future enhancements should focus on ensuring full system integration, particularly in non-clinical departments; establishing a documented disaster recovery plan; and adopting interoperable frameworks that support secure but efficient data exchange across systems and institutions. These strategies will not only enhance regulatory compliance and system reliability but also improve the quality, safety, and responsiveness of healthcare delivery.

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

Ultimately, a balanced approach that combines technological innovation, human-centered policies, and institutional governance is essential for building a digital health environment that is both secure and sustainable. By embracing this holistic vision, Puskesmas Sindangwangi can serve as a model for community-based health centers in Indonesia navigating the complex transition to digital systems in an increasingly connected world.

CONCLUSIONS

Puskesmas Sindangwangi has demonstrated a strong commitment to managing the security of Electronic Medical Records (EMR) by implementing the principles of confidentiality, integrity, and data availability, although it still faces some technical and operational challenges. The success of the EMR system can be enhanced by improving inter-unit integration, providing continuous training for human resources, and establishing formal policies for vendor management and disaster recovery plans to ensure the system's continuity and resilience. With these measures in place, Puskesmas Sindangwangi can create a safer and more efficient environment for managing health data, ultimately supporting the delivery of better healthcare services to the community.

AUTHOR CONTRIBUTIONS

[Fina Julia] played a pivotal role in the conceptualization and methodology of the research, as well as in data collection and analysis. [Dwi Ridho Aulianto] was responsible for the research design, methodological framework, and the subsequent analysis and interpretation of the data. Together, the authors collaborated closely to refine the research objectives and ensure a thorough review of the manuscript, enhancing its clarity and depth. Their joint efforts contributed significantly to the overall integrity and quality of the research presented.

CONFLICTS OF INTEREST

The authors declare that there are no conflicts of interest that could influence the outcomes of this research. No financial support or relevant personal relationships related to this article have been reported. All authors are committed to upholding the integrity of the research and ensuring that the findings presented are objective and free from external influences

FUNDING

This research did not receive any grants or financial support from any institution. All costs associated with the study were fully borne by the authors.

ACKNOWLEDGMENTS

We would like to express our gratitude to the informants who provided valuable insights during the interviews, which greatly enriched this research. Your contributions were instrumental in supporting the findings presented in this study.

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

REFERENCES

Amin, M., Setyonugroho, W., & Hidayah, N. (2021). Implementasi Rekam Medik Elektronik: Sebuah Studi Kualitatif. *Jatisi (Jurnal Teknik Informatika Dan Sistem Informasi), 8*(1), 430–442. https://doi.org/https://doi.org/10.35957/jatisi.v8i1.557.

Ardianto, E. T., & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, *3*(2), 18–30. https://doi.org/10.47134/rmik.v3i2.54.

Blake, L., Francis, V., Johnson, J., Khan, M., & McCray, T. (2017). Developing Robust Data Management Strategies for Unprecedented Challenges to Healthcare Information. *Journal of Leadership, Accountability and Ethics*, *14*(1), 22-31. Retrieved from https://articlegateway.com/index.php/JLAE/article/view/1611

Cellier, L., & Ghernaouti, S. (2019). An interdisciplinary approach for security, privacy and trust in the electronic medical record : A pragmatic legal perspective. *IEEE International Conference on E-health Networking, Application & Services (HealthCom)*, 1-6. Retrieved from https://ieeexplore.ieee.org/document/9009588/

Denkovski, V., Stojmenovska, I., Gavrilov, G., Radevski, V., & Trajkovik, V. (2024). Exploring current challenges on security and privacy in an operational eHealth information system. *Advances in Science, Technology and Engineering Systems Journal*. *9*(2). 45-54. Retrieved from https://www.astesj.com/v09/i02/p06/

Dias, F. M., Martens, M. L., Monken, S. F. de P., Silva, L. F. da, & Santibanez-Gonzalez, E. D. R. (2021). Risk management focusing on the best practices of data security systems for healthcare. *International Journal of Innovation*, *9*(1), 45–78. https://doi.org/10.5585/iji.v9i1.18246

Hartono, J. (2018). *Metoda Pengumpulan dan Teknik Analisis Data*. Yogyakarta : Penerbit Andi.

Indradi, Rano. (2020). *Rekam Medis*. Tangerang Selatan : Universitas Terbuka.

Ismatullah, N. K., Winarti, Y., Flora, H. S., Kusumaningrum, A. E., Syamsuriansyah, E., Silapurna, E. L., Amalin, A. M., Andriani, H., Surya, S., Yuliani, R. D., Husain, F. F., Reni Chairunnisah, Rahmawati, M. A., & Tambunan., C. A. (2023). *Rekam Medis.* Bandung: Widina Media Utama.

Izza, A. A., & Lailiyah, S. (2024). Kajian Literatur: Gambaran Implementasi Rekam Medis Elektronik di Rumah Sakit Indonesia berdasarkan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis. *Media Gizi Kesmas*, *13*(1), 549–562. https://doi.org/10.20473/mgk.v13i1.2024.549-562.

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

Joel, A. S., Abdussalaam, F., & Yunengsih, Y. (2023). Tata Kelola Rekam Medis Berbasis Teknologi Informasi Dalam Penanganan Kerahasiaan Dan Keamanan Data Pasien Dengan Metode Kriptografi. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *4*(3), 837–848. https://doi.org/10.35870/jimik.v4i3.287

Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, *3*(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Katsikas, S.K. (2013). Security of the Electronic Medical Record. In: Furht, B., Agarwal, A. (eds) Handbook of Medical and Healthcare Technologies. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-8495-0_18

Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis*. Jakarta: Kementerian Kesehatan. Retrieved from https://peraturan.go.id/id/permenkes-no-24-tahun-2022.

Kementerian Kesehatan Republik Indonesia. (2019). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 43 Tahun 2019 tentang Pusat Kesehatan Masyarakat*. Jakarta: Kementerian Kesehatan. Retrieved from https://peraturan.go.id/id/permenkes-no-43-tahun-2019.

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/10.1016/j.eij.2020.07.003.

Larasati, T., Fardiansyah, A. I., Saketi, D., & Nusa Dewiarti, A. (2024). The Ethical And Legal Aspects Of Health Policy On Electronic Medical Records In Indonesia. *Cepalo*, *8*(2), 103–112. https://doi.org/10.25041/cepalo.v8no2.3634

Mahendika, D., & Setyowati, M. (2023). Medical Record Digitization Policy: Overview of the Health Minister Regulation Number 24 of 2022. *Consilium Sanitatis: Journal of Health Science and Policy*, *1*(2), 54–61. https://doi.org/10.56855/jhsp.v1i2.227

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook. 3rd.* SAGE. Retrieved from https://books.google.co.id/books/about/Qualitative_Data_Analysis.html?id=3CNrUbTu6CsC&redir_esc=y.

Muljono, P., Sujana, J.G., & Prabowo, B. (2022). *Metodologi Penelitian Dan Laporan Kearsipan*. Tangerang Selatan: Universitas Terbuka.

Nisa, L., Sukaesih, S., & Saepudin, E. (2024). Pengelolaan Arsip Rekam Medis Elektronik di Klinik Pratama Unpad Singaperbangsa. *Innovative: Journal Of Social Science Research*, *4*(4), 711-726. https://doi.org/10.31004/innovative.v4i4.12893.

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

Ononiwu, C. C., & Mgbeafulike, I. J. (2024). Maintaining integrity and confidentiality of patients' records using an enhanced security technique. *International Journal of Innovative Science and Research Technology*. *9*(10). 1767-1773. https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

Pradita, R., Kusumo, R., & Rahmawati, R. (2022). Pentingnya aspek keamanan informasi data pasien pada penerapan RME di Puskesmas. *Journal of Sustainable Community Service*. *2*(2), 52-62. https://doi.org/10.55047/jscs.v2i2.437

Prayuti, Y. (2024). Implications of personal data protection law in consumer health data management to improve secure and confidential handling in Indonesia. *Jurnal Ius Constituendum*. *9*(3). 461-478. https://doi.org/10.26623/jic.v9i3.9289

Pujiarno, W. (2024). Analisa Yuridis Praktik Penggunaan Electric Informed Consent di Rumah Sakit Indonesia . *Majelis: Jurnal Hukum Indonesia*, *1*(3), 32–40. https://doi.org/10.62383/majelis.v1i3.18

Putrawansyah, A. P. B., & Sutabri, T. (2024). Analisis Keamanan Aplikasi Rekam Medis Elektronik Mengunakan Metode Penetration Testing pada UPTD RSD Besemah. *Router : Jurnal Teknik Informatika Dan Terapan*, *2*(4), 01–12. https://doi.org/10.62951/router.v2i4.268

Putri, R. D., & Mulyanti, D. (2023). Tantangan SIMRS dalam Penerapan Rekam Medis Elektronik Berdasarkan Permenkes 24 Tahun 2022: Literature Review. *Jurnal Medika Nusantara*, *1*(1), 18–28. https://doi.org/10.59680/medika.v1i1.288

Pratiwi, R., Utami, L. C., Sakti, R. B., & Triase. (2022). Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher. *Bulletin of Information Technology*, *3*(4), 367–373. https://doi.org/https://doi.org/10.47065/bit.v3i4.420

Shrivastava, U., Song, J., & Han, B. T. (2019). The implications of patient data security considerations for EHR interoperability and downtime recovery. Retreived from https://aisel.aisnet.org/amcis2019/treo/treos/68/

Suci, N. N., Nugroho, N. B., & Murniyanti, S. (2018). Implementasi Kriptografi Untuk Keamanan Data Rekam Medis Di Klinik Pratama Siti Rahmah Menggunakan Metode Advanced Encryption Standard. *Jurnal Cyber Tech*, *1*(10), 1–13. https://doi.org/10.53513/jct.v1i12.3622

Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif, Dan R & D*. Bandung : Alfabeta.

Tasbihah, F., & Yunengsih, Y. (2024). Penerapan Rekam Medis Elektronik dalam Menunjang Efektivitas Kerja Perekam Medis di Rumah Sakit Hasna Medika Cirebon. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*, *5*(3), 2761-2767. https://doi.org/10.35870/jimik.v5i3.946.

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518

Taufiq, A. R. (2019). Penerapan standar operasional prosedur (SOP) dan akuntabilitas kinerja Rumah Sakit. *Profita: Komunikasi Ilmiah dan Perpajakan*, *12*(1), 56-66. http://dx.doi.org/10.22441/profita.2019.v12.01.005

VanHoy, J. (2021). Third Party Risk Management. Social Science Research Network. Retreived form https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3763399

We'e, A., Nugroho, H., & Siswatibudi, H. (2023). Evaluasi Aspek Keamanan Dan Kerahasiaan Rekam Medis Elektronik Di Rumah Sakit Panti Nugroho. *Jurnal Permata Indonesia*, *14*(2), 72-81. https://doi.org/10.59737/jpi.v14i2.265.

Yunisca, F., Chalimah, E., & Sitanggang, L. O. A. (2022). Implementasi Peraturan Menteri Kesehatan Republik Indonesia Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis Terhadap Hasil Pemantauan Kesehatan Pekerja Radiasi di Kawasan Nuklir Serpong. *Reaktor : Buletin Pengelolaan Reaktor Nuklir, 19*(2), 34-41. https://doi.org/10.17146/bprn.2022.19.2.6700.

Zulkipli, F. N., Hussin, N., Yatin, S. F. M., & Ismail, A. (2022). Issues and trends of trusted mobile electronic medical records management for healthcare industry: A review. *International Journal of Business and Economy*, *4*(1), 50-59. Retrieved from http://myjms.mohe.gov.my/index.php/ijbec.

Cite this article: Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, *11*(1), 61-74. http://doi.org/10.14710/lenpust.v11i1.70518

E-ISSN: 2540-9638, ISSN: 2302-4666. © 2025 The Authors. Published by Universitas Diponegoro.
This is an open access article under the CC BY SA license (https://creativecommons.org/licenses/by-sa/4.0)
doi: http://doi.org/10.14710/lenpust.v11i1.70518