Research and Evidence on Knowledge in Administration and Management — Medical Electronic Data and Information Systems
Vol. 02, No. 2, September 2026, Page 16-31
E-ISSN 3123-6952

Healthcare Workers' Perception of Data Privacy in Cloud EMR Post Personal Data Protection Law

Telvie Kasenda[1]*, & Asmirati Yakob[2]
[1]*Universitas Klabat, Indonesia, [2]Politeknik Kesehatan Megarezky, Indonesia
*Co e-mail: telvie.kasenda@unklab.ac.id[1]

Article Information
Received: September 17, 2026
Revised: October 16, 2026
Online: October 31, 2026

Keywords
Data Privacy, Electronic Medical Records, Cloud, Personal Data Protection

ABSTRACT

The implementation of cloud-based electronic medical records (EMR) in hospitals brings changes in patient data management and raises new challenges related to data privacy following the enactment of Personal Data Protection Law (PDP Law) No. 27 of 2022. Medical records officers, who interact directly with patient data daily, have unique experiences regarding data privacy that remain underexplored, particularly in regional hospitals. This study aimed to explore the perceptions and experiences of medical records officers regarding patient data privacy in cloud-based EMR systems after the implementation of the PDP Law at RSUD dr. Rasidin Padang. A qualitative design with a descriptive phenomenological approach was employed. Seven active medical records officers with at least one year of EMR experience were selected through purposive sampling until data saturation was achieved. Data were collected through in-depth interviews, participatory observations, and documentation studies of data management SOPs and analyzed using the Colaizzi method. The findings revealed four main themes: dual awareness between work efficiency and data security concerns, limited understanding of regulations, the need for clearer technical guidelines and data privacy as a moral and professional responsibility. Medical records officers perceived data privacy as a moral and professional responsibility that was not fully supported by regulatory understanding. The study recommends contextual PDP Law training, strengthened technical assistance, and continuous evaluation of data privacy SOPs.

Keywords: *Data Privacy, Electronic Medical Records, Cloud, Personal Data Protection*

DOI: https://doi.org/10.69855/rekammedis.v2i2.873
Available online at website: https://gpijournal.com/index.php/rekammedis

This work is licensed under a Creative Commons Attribution 4.0 International license

INTRODUCTION

Digital transformation has fundamentally changed the way healthcare is managed around the world, including through the adoption of cloud computing technology in electronic medical record (EMR) systems. Cloud technology offers storage scalability, cost efficiency, and ease of access to real-time patient data from multiple locations and across healthcare facilities. This capability makes the cloud a strategic solution for hospitals to improve service quality while supporting coordination between medical personnel. However, behind these various advantages, new consequences also arise in the form of vulnerabilities to data security and privacy that must be seriously managed by every health facility (Syuhardi & Asmoro, 2024).

The vulnerability is even more apparent given that health data is classified as sensitive data that requires multiple layers of protection, while multi-tenant architecture in cloud environments increases the risk of leakage, unauthorized access, and misuse of patient personal information. Research in developed countries shows that healthcare users ' concerns about the privacy of their personal data on digital health portals are still high, even when systems are equipped with standard security mechanisms. This privacy issue not only concerns the technical aspects of the infrastructure, but also concerns the governance of access by multiple users in a single integrated EMR system. This condition confirms that the issue of data privacy in cloud-based EMR is cross-border and is a global concern in digital health governance (Keystone, Vehko, Jylha, & Kinnunen, 2024; Arvisais Anhalt et al., 2022).

Minister of Health Regulation No. 24 of 2022 requires all health facilities to migrate from manual medical record systems to EMR by the end of 2023, thereby accelerating the adoption of health information technology, including cloud infrastructure, in various types of hospitals. However, this massive and urgent migration is not balanced by adequate data security governance readiness, creating a gap between regulatory demands and security system readiness which is a critical point for the implementation of cloud-based EMR (Ministry of Health, 2022). This gap is even more relevant given the high incidence of ransomware attacks and data leaks in the global health sector, which makes this sector a prime target for cybercrime (Health-ISAC, 2024).

In Indonesia, the urgency is evident through several cases of large-scale health data leaks, such as the eHAC data leak on the Care Protect application and the leak of 19.5 million health data sold on hacker forums. These cases reveal weak data security governance in both government and private digital systems, as well as pushing public pressure for the government to strengthen the legal framework for personal data protection, especially in the health sector, which stores the most sensitive data (CNN Indonesia, 2023).

Responding to these needs, the government issued Law Number 27 of 2022 on Personal Data Protection (PDP law) as the first comprehensive legal framework in Indonesia, which places health data as special personal data with a higher level of protection, including data subject consent provisions, encryption, access rights, and incident handling procedures (Manurung & Thalib, 2022; Annan, 2024). However, the implementation of the PDP law in the health sector still faces obstacles, especially the lack of detailed implementing regulations and the absence of independent

This work is licensed under a Creative Commons Attribution 4.0 International license

supervisory bodies specifically for the health sector, so that compliance with the PDP Law is ultimately determined more by hospital internal policies and the readiness of officers who manage daily patient data (Heriyanto, 2023).

Health care workers, especially medical records officers, have a very important position in maintaining the privacy and security of patient data. This is because medical records officers are directly involved in various stages of data management, from the input process, storage, to the exchange of patient information through the EMR system. The level of competence and awareness of officers regarding the principle of confidentiality of information is one of the important aspects in determining the success of medical record data protection. Various studies on the safety of EMR in hospitals show that the human factor has a big role in maintaining information security. Officers' lack of understanding of privacy risks can increase the likelihood of data leakage caused by errors in carrying out procedures. Therefore, before assessing the success of a data security policy as a whole, it is important to know how medical records officers understand, view, and respond to patient data privacy issues (Ardianto, Sabran, & Nurjanah, 2024).

The importance of understanding the experience of officers is also supported by descriptive qualitative research conducted at Patju Gerung Hospital, West Lombok. The results showed that although hospitals have implemented user authentication and perform routine data backups every day, there are still obstacles in the competence of medical records officers and updates to Standard Operating Procedures (SOPs) related to data security. The study, which involved five informants through in-depth interviews and observations, showed that a qualitative approach can provide a deeper picture of the real conditions faced by officers in the implementation of data security. Through this approach, various aspects that are difficult to obtain only through quantitative methods, such as perceptions, concerns, experiences, and forms of adaptation of officers to policy changes, can be identified more comprehensively. The findings show that research on the experience and understanding of medical records officers is still relevant to be carried out in other regional hospitals that have similar characteristics (Fatuhu, M. S., dkk, 2025).

Within the scope of the province of West Sumatra, especially the city of Padang, the problem has relevance to the condition of digitizing health services at the regional level. Hospitals in Padang City have adopted the Electronic Medical Record (EMR) which is connected to the SATUSEHAT platform developed by the Ministry of Health. Despite this, the implementation process has not yet fully unfolded evenly. Of the ten Type C general hospitals in Padang City, there are still hospitals that have not met the completeness of data reporting through the system, one of which is RSUD dr. Rasidin Padang. This condition shows that the implementation of digitization of medical records at the regional level still faces various challenges, especially in aspects of governance and data management. Therefore, further studies are needed to understand how health care workers view and implement data privacy aspects in the use of the EMR system, especially after the enactment of the Personal Data Protection Law (Dinas Kesehatan Kota Padang, 2024).

This issue becomes even more relevant when it is associated with empirical findings in RSUD dr. Rasidin Padang, where a study on outpatient installations showed that 42.2% of health workers

This work is licensed under a Creative Commons Attribution 4.0 International license

expressed dissatisfaction with the EMR application used and 35.6% considered the EMR application still not good a paradox when faced with a relatively high infrastructure technical readiness score at the hospital. This gap between technical readiness and low user satisfaction cannot be adequately explained by the approaches that have dominated EMR data privacy and security studies in Indonesia, namely descriptive quantitative approaches and normative juridical studies that focus on regulatory compliance and infrastructure readiness, while the latest literature review confirms that EMR data interoperability and security challenges still require deep tracing that does not just rely on numerical data.

Such approaches tend to ignore the dimension of the subjective experience of the officer as the main actor implementing the system, when in fact the paradox between technical readiness and practical dissatisfaction can only be fully understood through the meaning and interpretation of the officer to the dilemma they face on a day to day basis between the demands of work efficiency and the, so the phenomenological approach is chosen as the most appropriate methodology because it is specifically designed to reveal the essence of the subject's lived experience in the face of complex and contradictory phenomena such as this. On that basis, this study intends to explore in depth the perception and experience of medical records officers related to patient data privacy in the cloud-based EMR system after the implementation of the PDP Law at RSUD dr. Rasidin Padang, in the hope that this holistic phenomenological understanding can explain why high technical readiness does not necessarily result in practical satisfaction and compliance, as well as provide more contextual operational recommendations to strengthen data privacy governance of electronic medical records in regional hospitals.

METHODS

This study uses a qualitative design with a descriptive phenomenological approach that aims to capture the meaning of informants' lived experiences informants related to patient data privacy in cloud-based EMR system after the implementation of the PDP Law. The study was conducted at RSUD dr. Rasidin Padang by considering the characteristics of the location as a regional hospital that has implemented EMR but still faces a gap between technical readiness and operational implementation. Informants were selected using purposive sampling with inclusion criteria were active medical records officer on duty at the RSUD dr. Rasidin Padang, has been using the EMR system for at least one year, is directly involved in the process of input, storage, or management of patient data, and is willing to become an informant voluntarily. Exclusion criteria are set for officers who are on sabbatical, do not want to be interviewed in depth, or have served less than one year so that they are not considered to have sufficient experience of the system. The number of informants were recruited at 7 people and can be increased or stopped according to the principle of data saturation, that is, when no new themes are found that arise from the interview.

Data collection was conducted through three complementary techniques, namely in-depth interviews using semi-structured interview guidelines that have been compiled based on literature reviews and validated through the assessment of two experts, namely an academic with a

This work is licensed under a Creative Commons Attribution 4.0 International license

background in health information management and an expert in qualitative research methodology, in order to ensure the accuracy of the substance of the question as well; and study of SOP data management documentation and Privacy Policy documents in force at the hospital. Research instruments in the form of researchers themselves as the main instrument (human instrument), assisted by interview guidelines, audio recording devices, field notes, and observation sheets. The interviews were conducted face-to-face at the informant's agreed place until they reached data saturation, then transcribed verbatim and analyzed with the Colaizzi method to identify meaningful themes. The validity and trustworthiness of the findings were established through triangulation of sources and methods, i.e. by comparing the results of interviews between informants and crossing them with participatory observation data and policy/SOP documentation, and through member checking, i.e. reconfirming the interpretation of key themes to informants to ensure compliance with their intended experience. The study also paid attention to the ethical aspects of the study by ensuring that each informant received a full explanation of the objectives, procedures, benefits, and risks of the study before signing info RSUD dr. Rasidin Padang consent as a form of voluntary participation agreement. The principle of confidentiality and anonymity of the informant's identity is maintained through the use of an initial code on all data and research results, while the informant remains entitled to resign from the study at any time without any consequences to his employment status.

RESULTS

Results of the Thematic Analysis Using the Colaizzi Method:

1. Theme 1: Dual Awareness Between Work Efficiency and Data Security Concerns

a. Understanding of Data Access.

All informants agreed that the cloud-based EMR system provides great convenience in accessing and distributing patient data between work units, so that the service process becomes faster than the previous manual system.

> *"Now find patient data faster, no need to disassemble physical files anymore."(P2)*

> *"The coding process becomes more efficient because patient history data can be accessed across time without having to wait for physical files to be sent from another room."(P5)*

b. Concerns About the Risk of Leakage and Unauthorized Access

Directly proportional to the convenience, almost all informants expressed concern about the potential for data leakage because the system was stored on servers that they could not physically or technically control.

> *"Patient data feels more accessible, but it's also easier to leak, because we don't know for sure who has access behind it."(P3)*

This work is licensed under a Creative Commons Attribution 4.0 International license

"I once felt misgivings when there was a system disruption, because I did not know whether patient data had been disclosed to outside parties during the disruption."(P6)

c. Ambivalence in Decision Making

This dual awareness gives rise to ambivalence when officers have to choose between speeding up services or slowing down the process for the sake of extra care in maintaining the privacy of patient data.

"I was once hesitant when asked to give quick access to those who claimed to be authorities, but did not bring complete official documents."(P1)

2. Theme 2: Limited Understanding of the PDP Act

a. Lack of Regulation Socialization at the Hospital Level

The majority of informants claimed not to understand in detail the substance of PDP Law No. 27 of 2022, especially regarding the rights of data subjects, obligations of data controllers, and legal consequences for violations, because socialization from the hospital is considered to be very limited.

"We heard the name of the law only, what kind of content has never been officially explained by the hospital."(P1)

"There is socialization, but it is occasional, not targeting directly to officers who work in the field like us."(P4, P7)

b. General Understanding, Not Specific Regulation

The informant's understanding of data privacy generally still rests on the principle of confidentiality of medical records in general taught since formal education, not on specific provisions in the PDP Law such as access rights, correction rights, or data subject complaint mechanisms.

"All I know is that medical records must be confidential, that's an old principle. When it comes to the PDP Law in detail, I don't understand it."(P5)

c. Individual Efforts to Seek Self-Understanding

Only one informant submitted an independent effort to understand the PDP Law outside the hospital's official program, but had difficulty relating the provisions of the law to his daily work practices.

This work is licensed under a Creative Commons Attribution 4.0 International license

"I have read the summary of the PDP Law on the internet out of personal curiosity, but it is difficult to relate it to my daily work in the coding section."(P5)

3. Theme 3: The Need for Clearer Technical and Training Guidelines

a. SOP That is Considered Not to Accommodate the PDP Act

All informants stated that the SOP for medical record management is currently still oriented to basic administrative procedures and does not contain an explicit reference to the provisions of the PDP Law. This was stated explicitly by one of the informants, as expressed in the following excerpt:

"The SOP that we hold is more about the procedures for filling out and storing files administratively, such as the numbering order or the procedure for borrowing medical records. Regarding the PDP, to be honest I have never seen it specifically mentioned in our SOP" (P3).

The statement illustrates that from the point of view of officials in the field, the existing SOP document has not accommodated the provisions on personal data protection as mandated by the PDP Law, but is still limited to purely technical-administrative aspects. The findings of this interview were also confirmed through the results of a documentation study, where no special clauses related to the handling of personal data in accordance with the PDP Law were found in the available SOP documents, so that there was a convergence between the perception of informants and the documentary evidence studied.

b. Technical-Applicative, Not Regulatory-Oriented Training

Some of the informants highlighted that the training they have received so far focuses more on how to operate EMR applications, not on the regulatory or ethical aspects of personal data protection.

"The training is more about how to input data correctly, not about how data privacy is regulated legally."(P4)

c. Vagueness of Incident Reporting Procedures

One of the informants highlighted the lack of a clear reporting path if the officer suspects an incident of leakage or unauthorized access to patient data.

"If, for example, we suspect that there is data leaking or accessed by unauthorized people, we ourselves still have doubts about who to report it to and through what channels."(P7)

4. Theme 4: Data Privacy as a Moral and Professional Responsibility

a. The Value of Professional Ethics as the Main Basis for Compliance

This work is licensed under a Creative Commons Attribution 4.0 International license

Apart from the limited understanding of regulation, all informants interpret the confidentiality of patient data as part of the moral responsibility and professional ethics that have been embedded since the education and professional oath of medical records.

> *"Maintaining patient privacy is an obligation from the heart, not because it is supervised or because there are laws."(P3)*

b. Internal Value-Based Compliance, Not the Threat of Legal Sanctions

In line with these statements, some informants affirm that their main motivation for maintaining data confidentiality is not due to fear of legal sanctions from the PDP Law, but rather because of a sense of responsibility for the trust of patients.

> *"I keep patient data not because I am afraid of being sanctioned by the law, but because it is the trust placed in them by patients."(P6, P1)*

c. The Gap Between Moral Values and the Strengthening of the Formal System

Although this professional moral value is an important capital, all informants realize that this value is not enough to ensure data security systemically without being supported by strengthening SOPs, training, and formal supervision from institutions.

> *"Good intentions are not enough if the system itself is not really ready."(P5)*

5. Essential Structure

Based on the integration of the four themes above, the essential structure of the experience of medical records officers at RSUD dr. Rasidin Padang can be formulated as follows: patient data privacy in a cloud-based EMR system is lived as a strong moral and professional responsibility and has been internalized during their formal professional education, but this appreciation goes hand in hand with the dual awareness between work efficiency and data security concerns, and has not been supported by an adequate understanding of PDP Law regulations or clear operational technical guidelines from the hospital. As the final stage of the *Colaizzi* method, the results of the thematic analysis are returned to all informants to confirm their suitability with the experience they convey. Six of the seven informants stated that the themes formulated had accurately represented their experiences, while one informant gave additional emphasis that aspects of the vagueness of incident reporting procedures needed to be highlighted more strongly.

DISCUSSION

The results of this study reveal that the perception of medical records officers on patient data privacy in the cloud-based EMR system at RSUD dr. Rasidin Padang is multidimensional, encompassing dual awareness between efficiency and security risks, limited understanding of PDP

This work is licensed under a Creative Commons Attribution 4.0 International license

Law regulations, the need for clearer technical guidelines, and the appreciation of privacy as a moral-professional responsibility. The four themes do not stand apart, but rather form a unified essential structure that influences each other in the day-to-day work practices of officers. This finding shows that compliance with data privacy at the operational level of regional hospitals is not solely determined by the existence of formal regulations, but also by internal factors such as professional values and external factors such as system support and institutional policies. The following discussion will outline each of these findings in more depth by linking them to related theories and research.

Theme 1: Dual Awareness Between Work Efficiency and Data Security Concerns

Informants' perception of the ease of data access through cloud-based EMR systems is in line with the characteristics of cloud computing technologies that enable centralized data storage and can be accessed elastically without relying on rigid physical infrastructure. This convenience provides tangible benefits for officers' work efficiency, especially in speeding up the process of searching and exchanging patient data between service units. This kind of efficiency benefit is a major reason why many healthcare institutions are adopting cloud-based storage models in their patient data management. However, the ease of access felt by officers in this study also shows that the benefit dimension tends to be more easily understood and perceived than the risk dimension which is latent and not always visible in daily work interactions (Fastekes IKTA, 2025).

The informant's concern about the risk of data leakage that arises along with the efficiency benefits can be explained through the framework of the privacy calculus theory, which states that individual decisions in sharing and managing personal data are the result of consideration between the benefits obtained and the perceived risks. In the context of this study, medical records officers implicitly performed similar calculations when they realized that the ease of work gained from cloud systems was directly proportional to the uncertainty about who actually had access to the data behind the system. A cross-cultural study of patients in China also found that perceived privacy risks and perceived benefits were both significant predictors of health data-sharing behavior. The suitability of these findings with the context of health care workers in Indonesia shows that the dynamics of privacy calculations not only apply to patients as data owners, but also to officers as parties who manage the data (Shi et al., 2023; Nainggolan, K., dkk, 2025).

Ambivalence experienced by officers in making work decisions, such as doubts about providing quick access without complete official documents, according to researchers indicates that officers actually have an ethical sensitivity to privacy issues, but this sensitivity has not been supported by clear authority and guidelines for making firm decisions. Researchers assume that this condition has the potential to cause inconsistency between officers and practices between situations, because the decision ultimately depends on the personal assessment of each individual in the field. In the absence of a standard frame of reference, this kind of ambivalence can be a weak point in the data security chain despite the officer's basically good intentions.

This work is licensed under a Creative Commons Attribution 4.0 International license

Theme 2: Limited Understanding of the PDP Act

Limited understanding of informants on the substance of PDP Law No. 27 of 2022 found in this study is in line with findings in various other health facilities in Indonesia, where patient data security policies have indeed been formally established through internal regulations, but their implementation at the operational level still requires strengthening, especially in standard procedures and data access management. The gap between the regulations that have been passed at the national level and the understanding at the field implementation level shows that the policy dissemination process has not been running effectively until it touches technical work units such as medical record installations. These conditions strengthen the argument that the existence of regulations without a structured socialization strategy tends to stop at the normative level and does not necessarily change the daily work practices of officers (Rusdiana, Utama, Sucipto, & Muhammad, 2024).

The understanding of informants who tend to rely on the principle of confidentiality of medical records in general, not on specific provisions of the PDP Law, also reflects the pattern found in legal studies on the urgency of the PDP Law in Indonesia, which highlights that public awareness and service actors of the existence and content of the PDP Law is still relatively low even though the regulation has officially entered into force. The principle of confidentiality of medical records that has long been taught in formal medical records education does provide a strong ethical foundation, but that foundation has not automatically included new technical provisions such as data subject rights, incident reporting obligations, or approval mechanisms specifically regulated in the PDP Law. This kind of knowledge gap confirms that regulatory transformation requires updating training curricula that not only repeat old principles, but also integrate new legal provisions (Lesmana, Elis, & Hamimah, 2022).

The individual effort of one of the informants to understand the PDP Law independently through searching for information on the internet illustrates the phenomenon of digital literacy that is personal and uneven among officers. This phenomenon is consistent with the study of personal data protection in the digital age which states that individual awareness of the importance of personal data often grows from personal initiatives due to the widespread reporting of data leakage cases, not from structured institutional learning programs. This kind of reliance on individual initiative risks creating a significant gap of understanding between officers in the same work unit. This condition further confirms the importance of the role of institutions in providing learning resources that are equal and accessible to all officers, not just depending on the personal motivation of each individual (Daeng, Linra, et al., 2023).

Researchers assume that the low understanding of regulation among medical records officers in this study is not due to lack of concern for privacy issues, but rather due to the lack of formal learning programs specifically designed to bridge between abstract legal regulations and concrete technical work practices. This assumption is reinforced by the finding that almost all informants continue to show high concern for data confidentiality despite their limited regulatory

This work is licensed under a Creative Commons Attribution 4.0 International license

understanding, which indicates awareness capital that can be further developed through appropriate interventions.

Comparison of the findings of this study with the results of measuring the readiness of RME implementation in RSUD dr. Rasidin Padang in the previous period showed a consistent pattern, namely that this hospital has technically and infrastructurally shown high readiness, but this readiness has not been followed by an equivalent maturity of understanding of data privacy regulations at the implementing officer level. The consistency of the findings between these periods shows that the problem of gaps in regulatory understanding is structural and has not experienced significant improvements even though the RME system has been running for several years. This indicates that the interventions that have been carried out so far are still focused on the technical-infrastructural aspects and have not touched the regulatory aspects and legal understanding adequately. This condition strengthens the urgency for hospital management to design capacity building programs that specifically target understanding of the PDP Law, not just technical training on system operation (Siswati, Muslimah, & Syafrawati, 2023).

Theme 3: The Need for Clearer Technical and Training Guidelines

The findings of the SOP on medical record management that has not accommodated the provisions of the PDP Act explicitly reinforce the results of previous research at hospital RSUD dr. Rasidin Padang, who measured the readiness of the EMR implementation using the DOQ-IT approach, where even though the readiness score for human resources and infrastructure is high, aspects of policy governance and SOPs still require further improvement. This conformity indicates that the SOP gap is not a new finding, but a problem that has been identified since the initial readiness phase of the EMR implementation but has not been fully addressed until the time of this study. This is also in line with the EMR implementation readiness study in the same hospital, which emphasizes that technical readiness and human resources do not necessarily guarantee the completeness of adaptive policy governance to regulatory changes. This condition shows a recurring pattern where national regulatory updates are often not followed in sync by updates to hospital internal policy documents (Susilo, Masdalena, Pramulichati, & Ihksan, 2024; Siswati, Muslimah, & Syafrawati, 2023).

The trend of training that is more technically-applicative oriented than the regulatory and ethical aspects of data privacy, as conveyed by informants in this study, is also found in research on training the use of EMR for medical personnel, which shows that the training provided generally focuses on increasing the confidence and effectiveness of the operation of the system, not on understanding the legal framework that accompanies it. This kind of training pattern is reasonable considering that the short-term urgency of institutions is more focused on smooth service operations than long-term regulatory compliance. Nevertheless, this dominance of technical orientation has the potential to create a competency gap, where officers are skilled at operating systems but lack understanding of the legal implications of any data management actions they perform. This gap can

This work is licensed under a Creative Commons Attribution 4.0 International license

ultimately increase the risk of data privacy violations that officers are not aware of as direct perpetrators (Burhan & Nadjib, 2024).

The vagueness of the reporting procedures for data leakage incidents submitted by one of the informants reinforces the findings of a systematic review of the security and privacy of RME data, which concluded that the weakness of the incident reporting mechanism is one of the most frequent vulnerable points found in health facilities in various countries, including Indonesia. Not only does this lack of clarity hinder rapid response to incidents, but it can also lead to under-reporting, where minor incidents go unreported because officers do not know the path or consequences of reporting. This condition is even more crucial considering that the PDP Law expressly requires data controllers to report data breach incidents within a certain period of time, an obligation that is difficult to fulfill if the internal reporting mechanism at the work unit level has not been properly established. This gap confirms that strengthening regulation at the macro level needs to be followed by strengthening technical mechanisms at the micro level of hospital operations (Ikawati & Ansyori, 2024).

The researchers assume that the three sub-findings on Theme 3 (SOP gaps, technical training orientation, and vagueness in incident reporting) are interrelated and reflect a common root problem, namely the lack of a framework for implementing the PDP Law that is thoroughly integrated into hospital operational governance. The absence of this implementation framework makes regulatory compliance a distributed and uncoordinated responsibility, so that each work unit has the potential to interpret and implement compliance differently according to their understanding.

Theme 4: Data Privacy as a Moral and Professional Responsibility

The appreciation of data privacy as a moral and professional responsibility found in all informants in this study is consistent with the study of ethical challenges in managing patient data in the era of digitization of health services, which confirms that ethical dilemmas in managing patient data cannot be solved only through regulatory approaches, but also require strengthening professional values in individual implementers. Moral values that have been internalized since the time of medical records education have become an important capital that distinguishes the officer's approach to data privacy from mere administrative compliance. However, the strength of these individual moral values can also be a double-edged sword if institutions rely too much on the personal values of officers without building a solid security system, because individual moral values cannot replace systemic control functions that are objective and consistent (Pongtambing & Sampetoding, 2023; Nainggolan, K., dkk, 2025).

The gap between the strength of individual moral values and the weakness of formal system strengthening revealed in Sub-theme 4.3 reinforces the findings of accredited laboratories and health facilities, showing that the highest information security risks often arise from aspects of managing organizational access and control, not from a lack of individual awareness. These findings confirm that data security and privacy are essentially the result of an interaction between human factors and

This work is licensed under a Creative Commons Attribution 4.0 International license

system factors, where weaknesses in one aspect can weaken the overall defense mechanism even though the other aspect is already strong. Thus, strengthening the moral values of medical records officers in hospitals dr. Rasidin Padang needs to be balanced with strengthening access control, information classification, and system supervision in parallel so as not to cause false sense of security at the individual level (Susanto & Legowo, 2023).

Overall, the results of this discussion confirmed that the perception of medical records officers on patient data privacy in the cloud-based EMR system at RSUD dr. Rasidin Padang is the result of a complex interaction between individual awareness, professional values, and institutional support systems that are not yet fully synchronized with each other. The researcher is of the view that strengthening data privacy in regional health institutions cannot depend only on formal compliance with national regulations or on individual moral values alone, but requires an approach that integrates all three aspects simultaneously. The phenomenological approach used in this study has succeeded in revealing dimensions of experience that have not been captured by quantitative and normative juridical approaches, thus providing a fuller understanding of how data privacy policies are actually carried out and interpreted at the level of real practice. These findings are an important foundation for the formulation of operational recommendations that are more contextual and based on the real needs of officers in the field.

CONCLUSIONS

This study revealed that the perception of medical records officers on patient data privacy in cloud-based EMR systems after the implementation of the PDP Law at RSUD dr. Rasidin Padang is formed by four main themes that are interrelated, namely the dual awareness between the demands of work efficiency and concerns about data security, limited understanding of the substance of PDP Law No. 27 of 2022, the need for clearer technical guidance and training, as well as the definition of data privacy as a moral responsibility as well as professional. Medical records officers live the ease of data access through the cloud system as a tangible benefit to service efficiency, but at the same time keep concerns about the risk of leakage and unauthorized access that is beyond their physical control. On the other hand, the officers' understanding of the PDP Law is still general and has not touched on specific provisions such as data subject rights, approval mechanisms, and incident reporting procedures, while the SOPs and training available are still technically-applicative oriented and have not explicitly accommodated the legal framework.

Based on these findings, operational implications that can be formulated for RSUD dr. Rasidin Padang include the development of contextual training modules that specifically bridge the substance of the PDP Law with the daily work practices of medical records officers, strengthening technical assistance that focuses not only on the operation of the system but also on understanding legal risks and responsibilities, as well as ongoing evaluation of data privacy SOPs to be in line with regulatory developments and field needs, including clarity of data leakage incident reporting mechanisms. This study has limitations that need to be considered in interpreting the results, among

This work is licensed under a Creative Commons Attribution 4.0 International license

others, the number of informants is limited to 7 people in accordance with the principle of phenomenological data saturation so that the findings are not intended to be generalized statistically to the population of medical records officers outside the research site, the nature of the study was only conducted, as well as the possibility of subjectivity bias in the process of interpretation of qualitative data even though member checks have been carried out to maintain the credibility of the results. Follow-up studies with a more extensive quantitative design or multi-site studies in several other regional hospitals are needed to more broadly test the representativeness of these findings, as well as to measure the effectiveness of the SOP training and reinforcement interventions recommended in this study.

ACKNOWLEDGMENT

The author would like to thank all those who have provided support in the process of research and writing this article. Thank you to all participants who have been willing to take the time to participate in this study.

REFERENCES

Annan, A. (2024). Tinjauan yuridis perlindungan data pribadi pada sektor kesehatan berdasarkan Undang-Undang No. 27 Tahun 2022. Sinergi: Jurnal Ilmiah Multidisiplin, 1(4), 247–254.

Ardianto, E. T., Sabran, & Nurjanah, L. (2024). Analysis of patient data security aspects in the implementation of electronic medical records at Hospital X. Jurnal Rekam Medik dan Manajemen Informasi Kesehatan (RAMMIK), 3(2), 18–30. https://doi.org/10.47134/rammik.v3i2.54

Arvisais-Anhalt, S., Lau, M., Lehmann, C. U., Holmgren, A. J., Medford, R. J., Ramirez, C. M., & Chen, C. N. (2022). The 21st Century Cures Act and multiuser electronic health record access: Potential pitfalls of information release. Journal of Medical Internet Research, 24(2), e34085. https://doi.org/10.2196/34085

Burhan, & Nadjib. (2024). Effectiveness of electronic medical record training among healthcare professionals. Sehat Rakyat: Jurnal Kesehatan Masyarakat, 3(3), 210–219.

CNN Indonesia. (2023, Januari). Leakage of 19.5 Million BPJS Ketenagakerjaan Records on a Hacker Forum. CNN Indonesia. https://www.cnnindonesia.com

CyberHub Indonesia. (2025). Surge in Cyberattacks: Indonesia Must Strengthen Health Data Regulations. CyberHub.id. https://cyberhub.id/berita/serangan-siber-ri-perkuat-regulasi

Daeng, L., et al. (2023). Personal data protection in the digital era: Challenges and its urgency in Indonesia. Meraja Journal, 6(2), 88–101.

eHealth.co.id. (2023). UU Personal Data Protection Law No. 27 of 2022 in the healthcare sector. eHealth Indonesia. https://ehealth.co.id/blog/post/uu-perlindungan-data-pribadi-no-27-2022-di-sektor-kesehatan/

This work is licensed under a Creative Commons Attribution 4.0 International license

Fakultas Teknologi Kesehatan. (2025). Patient data management using cloud computing technology. Fastekes IKTA. https://fastekes.ikta.ac.id/manajemen-data-pasien-dengan-teknologi-cloud-computing/

Heriyanto, H. (2023). A Comparative analysis of regulations and legal protection for patient data privacy in three Southeast Asian countries (Indonesia, Singapore, and Laos). Jurnal Ners, 7(2), 1247–1259.

Ikawati, F. R., & Ansyori, A. (2024). A systematic review of RME data privacy and security. Jurnal Manajemen Informasi Kesehatan Indonesia, 12(2), 210–222.

Fatuhu, M. S., Yanti, N. K. W., Septiana, A. P., & Khairani, F. (2025). A review of patient electronic medical record data security at Patut Patuh Patju Regional General Hospital, Gerung, West Lombok. *Jurnal Kesehatan Qamarul Huda*, *13*(2), 179-185. https://doi.org/10.37824/jkqh.v13i2.2025.1126

Hadjo, S., Dalimunthe, D.Y., Tasnim, T., Manalu, J.S., Sumiyati, I., Kasenda, T., Djuwadi, G., Sagala, N.S., Simamora, J.P., & Zainab, Z. (2025) Teori dan Praktik Promosi Kesehatan. Jakarta: Yayasan Kita Menulis.

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

Kyytsönen, M., Vehko, T., Jylhä, V., & Kinnunen, U. M. (2024). Privacy concerns among the users of a national patient portal: A cross-sectional population survey study. International Journal of Medical Informatics, 183, 105336. https://doi.org/10.1016/j.ijmedinf.2023.105336

Lesmana, C. T., Elis, E., & Hamimah, S. (2022). The urgency of the Personal Data Protection Law in ensuring personal data security as a means of fulfilling the right to privacy of the Indonesian people. Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, 3(2), 45–58. https://doi.org/10.52005/rechten.v3i2.78

Manurung, E. A. P., & Thalib, E. F. (2022). A juridical review of personal data protection under Law No. 27 of 2022. Jurnal Hukum Adigama, 5(1), 1–15.

Nainggolan, K., Panduwiyasa, H., Hasibuan, A., Ansya, Y.A., Fauziyyah, N., Sianturi, E., Dalimunthe, D.Y., Hadjo, S., Manoppo, I.J., & Sampouw, N. (2025) Promosi Kesehatan dan Ilmu Perilaku: Konsep dan Strategi. Jakarta: Yayasan Kita Menulis.

Nainggolan, K., Ansya, Y.A., Hamdayani, H., Sihombing, Y.A., Geneo, M., Hadjo, S., Rois, I., Siburian, U.D., Shidiq, A., & NNPS, R.I.N. (2025) Pengantar Ilmu Kesehatan Masyarakat di Era Global. Jakarta: Yayasan Kita Menulis.

Ombudsman RI. (2025). Ombudsman identifies maladministration at Dr. Rasidin Regional General Hospital and two Padang City Government agencies. Ombudsman Republik Indonesia Perwakilan Sumatera Barat. https://ombudsman.go.id/perwakilan/news/r/pwkmedia--ombudsman-temukan-maladministrasi-di-rsud-dr-rasidin-dan-dua-opd-pemko-padang

Pongtambing, Y. S., & Sampetoding, E. (2023). Ethical and patient data security challenges in the digitalization of healthcare services. Jurnal Presidensial (APPIHI), 2(1), 1–14.

This work is licensed under a Creative Commons Attribution 4.0 International license

Profil Kesehatan Kota Padang. (2024). Profil kesehatan Kota Padang tahun 2024. Dinas Kesehatan Kota Padang.

Rusdiana, I., Utama, T., Sucipto, & Muhammad, A. R. (2024). Analysis of patient data security policies at Hermina Serpong Hospital. Jurnal Manajemen Informasi Kesehatan Indonesia, 12(3), 145–155.

Shi, J., Yuan, R., Yan, X., Wang, M., Qiu, J., Ji, X., & Yu, G. (2023). Factors influencing the sharing of personal health data based on the integrated theory of privacy calculus and theory of planned behaviors framework: Results of a cross-sectional study of Chinese patients in the Yangtze River Delta. Journal of Medical Internet Research, 25, e46562. https://doi.org/10.2196/46562

Siswati, S., Muslimah, D., & Syafrawati. (2023). Analysis the readiness of implementing Electronic Medical Records (EMR) at dr. Rasidin Padang Regional Public Health Hospital. E3S Web of Conferences, 464, 06003. https://doi.org/10.1051/e3sconf/202346406003

Susanto, H., & Legowo, N. (2023). Information security risk analysis in clinical laboratories accredited to ISO 15189 and certified to ISO 9001. Jurnal Manajemen Informasi Kesehatan, 10(2), 247–253.

Susilo, H., Masdalena, Pramulichati, S., & Ihksan, M. (2024). Assessing the level of preparedness for electronic medical record system implementation using the DOQ-IT approach at Dr. Rasidin Regional General Hospital, Padang. Journal of Medical Records and Health Information (JRMIK), 5(1), 13–22.

Syuhardi, Y. I., & Asmoro, E. T. (2024). Cloud computing security: Challenges and solutions. Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research, 1(4), 1997–2004. https://doi.org/10.32672/mister.v1i4.2171

Vettha, I., Widasari, S., Ikawati, F. R., & Syukron, A. (2025). Literature review: Challenges of electronic medical record interoperability in healthcare facilities. Jurnal Kesehatan Tropis Indonesia, 4(3), 417–427.