Jurnal Iman dan Spiritualitas
eISSN: 2775-4596, Vol 6, No 4, 2026, pp. 1709-1722
https://doi.org/10.15575/jis.v6i4.58527

Legal Analysis of Electronic Medical Record Interoperability with the SATUSEHAT Platform: A Case Study of Padjajaran Network Clinic

Tya Amelia
Universitas Islam Nusantara Bandung, Indonesia
Amelyatya89@gmail.com

Suggested Citation:

Amelia, Tya. (2026). Legal Analysis of Electronic Medical Record Interoperability with the SATUSEHAT Platform: A Case Study of Padjajaran Network Clinic. *Jurnal Iman dan Spiritualitas*, Volume 6, Number 4: 1709–1722. https://doi.org/10.15575/jis.v6i4.58527.

Article's History:

Received August 2026; *Revised* September 2026; *Accepted* October 2026.
2026. journal.uinsgd.ac.id ©. All rights reserved.

Abstract:

Indonesia's healthcare sector is undergoing a major digital transformation with the introduction of SATUSEHAT, a national platform designed to unify patient data and enable interoperability among health facilities. The enactment of Permenkes No. 24/2022 on Medical Records has made electronic medical records (EMRs) mandatory and requires their integration with SATUSEHAT, supported by broader regulations such as the Health Law and the Personal Data Protection Law (UU No. 27/2022). This article examines the legal framework governing EMR–SATUSEHAT integration and analyzes its real-world implementation in Klinik Jejaring Padjadjaran (KJP), a network of primary care clinics in West Java. Using a mixed-method approach, doctrinal legal analysis of statutes and regulations, alongside a qualitative case study of KJP's implementation, the study explores compliance challenges, legal risks, and practical benefits. Findings indicate that while KJP achieved regulatory compliance through system upgrades, data standardization, interoperability testing, and reinforced privacy safeguards, the process required significant investment in resources and staff training. The case highlights tensions between older regulations and new integration mandates, as well as the need for further clarity on patient consent under the data protection regime. Ultimately, KJP's experience illustrates both the opportunities and complexities of Indonesia's digital health transformation, offering a model for other healthcare providers navigating EMR interoperability and data governance.

Keywords: data privacy; Electronic Medical Records (EMR); health law; interoperability; legal review; personal data protection.

INTRODUCTION

Digital transformation in the healthcare sector is one of the Indonesian government's strategic agendas to improve service quality, expand access, and strengthen national healthcare system governance. This shift aligns with global trends in which digitalization is the foundation of modern healthcare systems, particularly in the use of electronic medical records, health big data, and interoperable platforms that integrate health data across facilities (Osborn et al., 2022). In the Indonesian context, one of the most significant innovations is the launch of SATUSEHAT, an integrated platform developed by the Ministry of Health to unify patient data nationally and build a more comprehensive, efficient, and secure digital health ecosystem. SATUSEHAT is designed as a National Health Information Exchange (NHIE) that utilizes the global interoperability standard, Health Level Seven–Fast Healthcare Interoperability Resources (HL7 FHIR). This standard enables real-time, structured, and consistent exchange of clinical data across multiple health information systems and healthcare facilities (Xiao et al., 2021). By using HL7 FHIR, Indonesia is following international best practices in electronic medical record integration, as adopted by

countries with advanced digital health systems including the United States, the United Kingdom, and Australia (Bender & Sartipi, 2013). The use of this global standard not only improves data quality but also accelerates interoperability across facilities, ultimately driving improved clinical decision-making and patient safety.

As a follow-up to this initiative, the Indonesian government, through various legal instruments, mandated all healthcare facilities to adopt Electronic Medical Records (ERCs) and integrate them with the SATUSEHAT platform. This regulation is further reinforced by Minister of Health Regulation Number 24 of 2022 concerning Medical Records, which stipulates that all healthcare providers must ensure that their EMRs meet interoperability standards and are connected to SATUSEHAT as part of the national digital health ecosystem (Julia & Aulianto, 2025). This policy stems from the primary need for the Indonesian healthcare system to address data fragmentation, information duplication, and inconsistencies in clinical documentation, which have historically hindered clinical decision-making and public health planning (Setyani & Mahendro, 2025).

In the context of policy implementation, the Padjadjaran Network Clinic (KJP) can be seen as a concrete example of digital transformation at the primary care level. KJP is a network of primary healthcare clinics affiliated with Padjadjaran Regional Hospital in West Java and comprises more than ten clinics spread across various districts/cities. Prior to its integration with SATUSEHAT, KJP had developed an internal digital system to manage medical records, patient administration, and clinical services in an integrated manner. However, the national digital transformation prompted this clinic network to adapt its system, particularly to ensure that its EMR meets HL7 FHIR interoperability standards and is capable of real-time communication with SATUSEHAT (KJP, 2024).

The integration of the KJP EMR system with SATUSEHAT reflects a broader dynamic within the Indonesian healthcare system, namely a shift in the health law paradigm toward a stronger emphasis on data integration, interoperability, information security, and privacy protection. This development aligns with the enactment of Law Number 17 of 2023 concerning Health, which provides a stronger legal basis for the digitalization of technology-based health services and data management (Naili et al., 2024). Furthermore, the 2022 Personal Data Protection Law (PDP Law) is a crucial instrument in ensuring the security and privacy of highly sensitive digital health data (Khanna & Kotwal, 2025). In an increasingly complex data ecosystem, protecting data subjects' rights is a key pillar to ensure that digital transformation does not conflict with the principles of medical ethics or the fundamental rights of citizens.

While digital transformation offers significant opportunities, the RME–SATUSEHAT integration process is not without challenges. Technically, healthcare facilities face issues related to data format compatibility, internal system unpreparedness, software vendor variations, and limited digital infrastructure in some regions (Muinga et al., 2020). Institutionally, adjustments to standard operating procedures, human resource training, and the development of an organizational culture that supports consistent RME use are required (Nurmaidah et al., 2024). Regulatory-wise, healthcare facilities must navigate various legal provisions related to data storage, information accessibility, patient consent, and legal liability in the event of data breaches or system failures (Goswami & Mondal, 2025).

Through a case study of KJP, this article seeks to provide an in-depth analysis of the legal framework governing the integration of Electronic Medical Records (EMR)—specifically within the SATUSEHAT ecosystem—in Indonesia, and to examine its implementation at the primary healthcare level. This analysis focuses on two key areas. First, it reviews core health sector regulations, particularly the Minister of Health Regulation (Permenkes) No. 24/2022 concerning Medical Records, which establishes the legal basis for the use and integration of EMR (Asyfia et al., 2023). This regulation reaffirms the obligation of healthcare facilities to maintain the confidentiality of medical records, ensure data quality, and implement interoperability standards established by the government. The Ministry of Health regulation serves not merely as an administrative instrument, but also as a reflection of the national policy direction to position health data as a strategic asset that must be managed in a secure, structured, and integrated manner.

Second, a review of laws governing data protection and information security, particularly the 2023 Health Law and the 2022 Personal Data Protection Law (Sarabdeen & Mohamed Ishak, 2025). These two laws influence how healthcare facilities manage sensitive patient data, ensure the validity of consent, establish access control mechanisms, and determine legal liability in the event of a security incident. In the digital era, data privacy and security issues are increasingly receiving public attention. Therefore, the integration of RME–SATUSEHAT must align with the principles of lawful processing, data minimization, and purpose limitation as stipulated in international data protection standards (Faisal, 2023).

This study not only assesses KJP's compliance with these various regulations but also examines the real challenges faced in the integration process. Based on policy documents, field observations, and interviews with KJP healthcare workers, the study evaluates several aspects, such as information technology readiness,

healthcare worker training mechanisms, coordination with information system vendors, and potential legal risks arising from clinical data interoperability. Furthermore, the benefits gained from the integration are also examined, such as service efficiency, increased diagnostic accuracy, improved patient monitoring capabilities, and ease of data access by authorized healthcare workers.

Ultimately, the discussion of the RME–SATUSEHAT integration in the KJP case provides important insights into how digital transformation in Indonesia's healthcare sector is unfolding on the ground. The findings from this case position digital system integration not merely as a technical issue, but as a legal, ethical, and governance issue that requires a comprehensive approach. Health digitalization is merely a tool; its effectiveness depends heavily on regulatory readiness, institutional capacity, human resource competency, and a commitment to protecting patient rights.

Therefore, this research contributes in two main aspects: first, it enriches the literature on health data integration in the context of developing countries; and second, it provides practical recommendations for health facilities, policymakers, and other stakeholders in strengthening digital health information governance in Indonesia. Therefore, this study is expected to support a sustainable, inclusive digital transformation process oriented towards improving the quality of national health services.

METHOD

This study uses a mixed-methods approach designed to provide a comprehensive understanding of the dynamics of electronic medical records (EMR) regulations and their implementation in practice at healthcare facilities, particularly in the context of the integration of the SATUSEHAT system at the Padjadjaran Network Clinic (KJP) (Creswell & Creswell, 2018). A mixed-methods approach was chosen because the issue of health data governance is multidimensional: on the one hand, it demands rigorous textual analysis of the applicable legal framework; on the other hand, it also requires an empirical understanding of how regulations are translated into operational practices on the ground. The combination of these two approaches allows the study to explain the gap between legal norms and actual practice, a problem often highlighted in digital health policy studies. Therefore, the methodological design in this study is not only descriptive, but also interpretive and evaluative.

The first stage of the research was conducted through doctrinal legal research, which focused on a systematic review of the laws, government regulations, and technical regulations that form the basis for the implementation of EMR and health data governance in Indonesia (VanGestel & Micklitz, 2011). The doctrinal approach was chosen because it prioritizes analysis of the content of positive law, normative structures, relationships between regulations, and the legal principles underlying health data regulation. This method is widely used in digital health law research to assess regulatory coherence, policy consistency, and the level of legal certainty for healthcare providers.

The analysis begins with statutory regulations, namely Law No. 36 of 2009 concerning Health, which stipulates the obligation of health care facilities to maintain complete and accurate medical records as part of service standards (Kementerian Kesehatan, 2009). Furthermore, this study examines Law No. 29 of 2004 concerning Medical Practice, specifically the provisions regarding the obligations of medical personnel in recording, storing, and maintaining the confidentiality of medical records (Kementerian Hukum dan HAM, 2004). These two laws serve as the primary normative basis governing the functions, responsibilities, and minimum standards for maintaining medical records, both in conventional and electronic formats.

At the technical regulatory level, the research examines in-depth the Minister of Health Regulation No. 24 of 2022 concerning Medical Records, a regulation that serves as the foundation for the national digital transformation of health, including the integration of EMR with the SATUSEHAT platform. This Minister of Health Regulation regulates key aspects such as interoperability standards, data formats, access and authorization mechanisms, security and confidentiality principles, and healthcare facility obligations in data integration. Furthermore, regulations regarding the implementation of electronic systems are also reviewed through official documents from the Ministry of Communication and Informatics, particularly those related to the classification of strategic electronic systems and the obligation to conduct system security audits.

The legal analysis was further expanded by examining Law No. 27 of 2022 concerning Personal Data Protection (PDP), which establishes fundamental principles of data protection, including the basis for data processing, data subject rights, data controller obligations, and mandatory security standards (Kementerian Kominfo, 2022). Health data is categorized as sensitive personal data, thus applying stricter protection standards, particularly regarding its storage, access, and use. All of these provisions were used to develop an analytical framework for assessing the compliance of RME practices at the Padjadjaran Network Clinic with regulatory mandates.

RESULTS AND DISCUSSION

A Doctrinal Legal Analysis of the Regulatory Framework for Medical Records and Data Governance in Indonesia

This study employs a doctrinal legal approach to systematically, critically, and comprehensively examine all legal norms that form the regulatory framework for medical records and health data governance in Indonesia (Darnela & Rusdiana, 2025). This approach is crucial because the issue of electronic medical records (EMR) and the integration of the national health system through SATUSEHAT lies at the intersection of health law, personal data protection law, and national digital policy. Doctrinal analysis is used not only to identify applicable normative rules but primarily to understand how these norms shape the boundaries of the authority, obligations, and legal responsibilities of healthcare facilities in managing patient data (NE Varuhas, 2023). Therefore, this approach is not merely descriptive but also evaluative in its assessment of regulatory coherence, harmonization, and adequacy.

The primary regulatory basis focused on in this study is Law No. 36 of 2009 concerning Health, which affirms that individual health information is a fundamental patient right that must be protected by the state (Sijabat & Tridewiyanti, 2022). This law positions medical records as a crucial legal instrument for ensuring the quality of healthcare services, providing legal evidence, and protecting patient rights. The articles concerning health data confidentiality in the Health Law serve as a starting point for understanding the obligations of healthcare facilities to maintain data integrity, security, and confidentiality (Hulkower et al., 2020). This provision becomes even more significant in the context of the digitalization of healthcare services, which allows patient information to potentially move more quickly and widely through national electronic systems.

Furthermore, this study examines Law No. 29 of 2004 concerning Medical Practice, which provides stricter regulations regarding the obligation to maintain medical records by medical personnel (Hariharan et al., 2006). Article 46 stipulates that every doctor and dentist is required to create complete, accurate medical records, and store them in accordance with the provisions of medical professional confidentiality (Sugiarti, 2020). This law also regulates the legal consequences if medical personnel or health care facilities fail to maintain the confidentiality of medical records, thus emphasizing the aspect of legal accountability in health data governance. Analysis of the Medical Practice Law shows that medical records are not merely administrative documents, but legal artifacts that have direct implications for aspects of professional ethics, litigation evidence, and patient legal protection.

In terms of technical implementation, this research focuses on Minister of Health Regulation No. 24 of 2022 concerning Medical Records, which provides an operational framework for the implementation of electronic medical records (EMD). This regulation introduces national interoperability standards, data security provisions, and requires every healthcare facility to integrate with the SATUSEHAT platform (Arabi et al., 2022). The regulation stipulates that electronic medical records must meet the principles of availability, confidentiality, and integrity, and be equipped with an audit mechanism to ensure accountability (López, 2020). This regulation can be seen as a milestone in the modernization of Indonesia's healthcare system, but it also raises questions about the readiness of the infrastructure, human resources, and technical capacity of small and medium-sized healthcare facilities—including the Padjadjaran Network Clinic—to meet these national standards.

The doctrinal study was then expanded by examining Law No. 27 of 2022 concerning Personal Data Protection (PDP), which serves as the primary reference for individual data protection in Indonesia, including health data, which is classified as sensitive personal data (Lestari & Rasji, 2024). The PDP Law provides a stronger legal basis for data subject rights, data controller and processor obligations, and law enforcement mechanisms for data leaks or misuse. From this research perspective, the PDP Law is a key regulation because the integration of RME into SATUSEHAT expands the flow of patient data across institutions, increasing the risk of security breaches. This study analyzes how the PDP Law regulates the principles of lawfulness, purpose limitation, data minimization, and accountability, and how these principles should be translated into internal policies and technical procedures of healthcare facilities.

The doctrinal analysis also includes derivative regulations and technical guidelines from the Ministry of Health and the Ministry of Communication and Informatics, particularly regarding the implementation of electronic systems and information security standards (Yeng et al., 2022). Documents such as the Information Security Management System (ISMS) guidelines and risk assessment mechanisms in healthcare facilities are reviewed to understand how national policies translate the principles of the law into operational instruments. Regulations regarding electronic system operators (ESOs) are relevant given that healthcare facilities, including KJP, in practice act as electronic system operators and are required to meet minimum standards for security, encryption,

access control, and incident reporting. A doctrinal approach allows researchers to assess whether these standards are realistic and proportionate when applied to healthcare facilities with limited capacity (Benneh Mensah & Dutta, 2024).

Through this analysis, the research identified tensions between the overarching goal of national health data and personal data protection, particularly in the context of mandatory integration with government platforms. On the one hand, digitalization through SATUSEHAT offers efficiency, interoperability, and improved quality of data-driven services. However, on the other hand, this integration carries the risk of concentrating sensitive health data in a single central system that is not yet fully guaranteed by independent and robust oversight mechanisms. Policy literature indicates that centralizing health data within a national system requires a strict governance framework to prevent misuse and data overreach by the government or third parties (Isibor, 2024).

A doctrinal legal approach was also used to assess the alignment and harmonization between health regulations and data protection regulations. This study found that although the PDP Law provides a fairly robust data protection framework, several provisions in Ministerial Regulation 24/2022 still leave considerable room for interpretation for the government in accessing patient health data (Schmidt et al., 2024). For example, the concept of "public service needs" in the Ministerial Regulation is not strictly defined, potentially conflicting with the purpose limitation principle in the PDP Law (Forgó et al., 2017). This normative misalignment has a direct impact on healthcare facilities, as they are forced to comply with two regulatory regimes simultaneously without adequate harmonization guidelines. This study used a doctrinal approach to uncover these contradictions and assess the extent to which regulations can provide legal certainty for healthcare facilities such as KJP.

Thus, the doctrinal legal analysis in this study provides a strong conceptual foundation for understanding how legal regulations regulate, limit, and guide the digitization of medical records in Indonesia (Tilaar & Sewu, 2023). The results of this analysis serve as the basis for the next section, which will assess how the Padjadjaran Network Clinic implements these regulations in practice, as well as the extent to which existing regulations support or hinder the integration of RME with SATUSEHAT.

Qualitative Case Study of Padjadjaran Network Clinic (KJP)

Early in implementation, there was resistance due to the increased administrative workload, particularly during the transition phase when manual and electronic systems were still running simultaneously. This obstacle aligns with previous research findings showing that digital transition fatigue often occurs in healthcare facilities with limited resources (Kovan, 2025). However, with training and familiarization, administrative staff began to see the system's benefits, particularly in speeding up medical record searches and reducing recording errors.

Analysis of training records and internal outreach materials indicates that KJP is attempting to implement a phased approach to RME implementation. Training is conducted in several waves, focusing on three aspects: (1) technical knowledge of system usage, (2) understanding of RME regulations and obligations to maintain patient privacy, and (3) data breach risk management. Training materials emphasize the importance of compliance with the Personal Data Protection Law and Minister of Health Regulation No. 24 of 2022, particularly the principles of confidentiality and access control. This phased training approach demonstrates that KJP recognizes that digital transformation is not only a technological change, but also a change in work culture (Tourani et al., 2018).

Another important finding is how KJP adjusted its internal policies to comply with legal requirements. For example, in response to data confidentiality obligations, the clinic issued a new data governance policy that governs procedures for access, storage, destruction, and reporting of data security incidents (Al-Ruithe et al., 2019). KJP also established a password policy, a ban on the use of personal devices to access the clinic's systems, and a periodic audit log procedure to track user activity (Fitri et al., 2025). This demonstrates that regulatory implementation extends beyond system operation to internal governance focused on accountability and risk mitigation. These practices align with recommendations in the literature on organizational compliance in the digital health sector.

The case study data also revealed the dynamics of the KJP registration process on the SATUSEHAT platform as an Electronic Medical Record Operator (EMRO). This process involved fulfilling quite complex administrative requirements, such as verifying the clinic's legality, auditing system feasibility, and evaluating information security standards (Mahmoudi et al., 2020). This process took longer than expected because some documents required revisions to comply with the Ministry of Health's format and standards. This delay highlights the compliance burden on health facilities with limited resources and reinforces the argument that national digital policies need to consider disparities in readiness across health facilities (Engle et al., 2023).

An analysis of KJP's public communications—including social media, information brochures, and official announcements—shows that clinics strive to build positive patient perceptions regarding the use of EMR. Public communications focus on benefits such as speed of service, accuracy of recording, and connectivity with referral hospitals (Prang et al., 2018). However, KJP's public communications have not fully educated patients about how their data is managed, security risks, and their rights as data subjects. This is despite the PDP Law requiring healthcare facilities to provide clear information about the purpose of data collection, protection mechanisms, and rights to access and correct data. This gap is a crucial finding because it demonstrates that regulatory compliance is not merely technical and administrative but also relates to transparency with the public.

Nevertheless, this case study also shows that KJP successfully achieved several positive outcomes from its RME implementation. These include improved consistency of clinical records, easier access to medical records across units, and increased efficiency of service processes. The electronic system also helped the clinic more accurately identify patient visit patterns and service needs, which are crucial for developing a data-driven service strategy (Lyu, 2025). Thus, although its implementation faced several obstacles and required significant adjustments, the digital transformation at KJP brought positive changes relevant to improving service quality.

Based on the overall data, this study identified four main barriers to the implementation of RME and SATUSEHAT in the KJP: limited technical capacity, initial resistance, complex administrative requirements, and lack of public education. These four barriers confirm that the digital divide in healthcare exists not only among users but also among healthcare providers (Saeed & Masters, 2021). Before presenting a table summarizing these findings, the following section provides a key insight into how each barrier interconnects and shapes organizational adaptation patterns in the KJP.

Table 1 Summary of Barriers, Adaptation Strategies, and Results of RME & SATUSEHAT Implementation in KJP

Category	Key Findings	Analytical Description
Technical Barriers	Initial infrastructure & technical capability limitations	EMR systems require stable devices and networks, while the technical capacity of clinic staff and equipment is limited. This slows the adoption process and leads to transition fatigue.
Organizational Barriers	Staff resistance in the transition phase	Staff experienced increased workloads due to the simultaneous use of manual and electronic systems. Resistance decreased after gradual training.
Regulatory & Administrative Barriers	The complexity of EMRO SATUSEHAT registration requirements	The registration process requires legal verification, security audits, and compliance with strict technical standards. Documents require repeated revisions, creating a compliance burden.
Barriers to Public Communication	Lack of patient education regarding data privacy and rights as data subjects	Clinical communications highlight the benefits of RME, but do not yet include detailed explanations of data management, privacy protection, and the right to correction and access to data under the PDP Law.
Technical Adaptation Strategy	Modernization of recording procedures & system integration	The clinic is gradually shifting processes from manual to digital while ensuring interoperability with SATUSEHAT for referral services.
HR Adaptation Strategy	Gradual training and digital literacy improvement	Training focuses on technical, regulatory, and data security aspects. The phased approach reduces resistance and increases staff digital confidence.
Data Governance Strategy	Formation of new internal policies	The clinic establishes a password policy, audit log procedures, personal device restrictions, and standard operating procedures for data storage and destruction. This demonstrates substantive compliance, not just normative compliance.

Public Communication Strategy	Communicating the benefits of RME through social media & brochures	It focuses on service speed, accuracy, and connectivity, but fails to adequately incorporate patient rights and data protection mechanisms.
Implementation Results – Service Efficiency	Improved access speed and recording consistency	Electronic systems speed up medical record searches, reduce recording errors, and facilitate coordination between units.
Implementation Results–Data-Driven Approach	Analytical capabilities to map visiting patterns	RME enables the identification of case trends and service needs, which is useful for data-driven clinical strategy development.
Implementation Results–Regulatory Compliance	Internal governance is increasingly strong and documented	The implementation of regulations encourages the establishment of a more accountable and standardized data security system in accordance with the PDP Law and the Minister of Health Regulation.

The table more systematically demonstrates how various barriers, adaptation strategies, and implementation outcomes are interconnected in the digital transformation process at KJP. The technical and administrative barriers identified in the initial phase, for example, were not isolated but closely related to the organization's low readiness for change in infrastructure and biometrics. This situation confirms that the success of RME implementation is determined not only by system availability but also by the alignment between technology, regulations, and institutional capacity (institutional readiness). This is further reinforced by the fact that after gradual training, staff resistance diminished, and the system's benefits became more apparent (Webster & Gardner, 2019).

The data governance strategy developed by KJP, including internal policies related to access and security, demonstrates a significant shift from mere normative compliance to substantive compliance. By strengthening internal accountability structures, KJP demonstrates that regulation can be a tool for improving organizational quality, not simply a compliance checklist (Kulp et al., 2020). However, findings regarding the lack of public education on data privacy indicate that digital transformation has yet to address the dimensions of patient participation and literacy, crucial under the PDP Law.

The table also shows that despite significant challenges, KJP was able to achieve several positive outcomes, such as consistent recording, speed of service, and data-driven analytical capabilities. The system's ability to identify patient visit patterns provides opportunities for the development of data-driven healthcare planning (Helén & Tarkkala, 2024). These findings demonstrate that digital transformation not only increases efficiency but also opens up opportunities for data-driven innovation as the foundation for future primary healthcare services.

Conceptually, the results of this study demonstrate that the implementation of digital health regulations at the primary care facility level cannot be understood solely as a technical process, but as an organizational adaptation process involving a dynamic interaction between regulations, human resources, technology, and public communication (Jimenez et al., 2020). Thus, the KJP case study provides an empirical overview of how national policies operate at the most micro-level, while also revealing gaps that must be addressed to achieve an inclusive and sustainable digital health ecosystem.

KJP Privacy Policy Reform, Patient Consent, and Compliance Challenges

The privacy policy reform within the Jakarta Cares Area (KJP) program and its integration with the SATUSEHAT system is a crucial milestone in the restructuring of public health data governance in Indonesia. This change is driven not only by digital technocracy but also by legal obligations, particularly following the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which requires all data managers to update their policies, standards, and practices for collecting and processing personal data. In this context, the KJP privacy policy reform should be understood as a structural response to increasingly stringent legal requirements, as well as an effort to increase public legitimacy of the increasingly digitalized healthcare

system. As highlighted in data governance studies, organizations facing new regulatory regimes tend to reform their privacy policies to align with the principles of lawful, fair, and transparent processing (Custers et al., 2019).

One fundamental aspect of the privacy policy update is the privacy notice mechanism, which obligates governments or healthcare facilities to provide clear, understandable, and accessible notices to patients. Privacy notices must include the legal basis for data processing, the intended use, the third parties receiving the data, the retention period, and the rights of the data subject (Lubello & Vedaschi, 2015). Within the KJP ecosystem, this notice holds a strategic position as it serves as a prerequisite for legitimizing the processing of sensitive health data. Based on the PDP Law, which adopts the principle of informed consent, notice is considered a moral pillar for reducing information asymmetry between the state and citizens (Pallocci et al., 2023). Without complete and adequate notice, the relationship between patients and healthcare providers has the potential to create a form of invisibility that threatens public trust.

From the privacy notice, the next, more technical but crucial issue is explicit consent. Health data is categorized as special personal data, so its processing requires explicit, documented, and traceable consent. The new regime requires the KJP to design a consent format that not only meets legal requirements but also facilitates the process for patients to grant, withdraw, or restrict consent. Literature on health data governance shows that a consent mechanism that can be withdrawn at any time is a crucial principle in protecting patient autonomy (Vedder & Spajić, 2023). In practice, KJP administrators must have a consent storage system integrated with patient identity for easy auditing and to ensure that withdrawals are effectively implemented—meaning data is no longer processed after consent is revoked.

Complexity increases when it comes to tagging sensitive data, particularly information related to HIV/AIDS, mental health, and reproductive health. These three categories of data require extra protection due to the potential for social stigma, discrimination, or serious psychological impacts if leaked. According to sensitive data governance research, granular tagging allows systems to limit access to specific information based on clinical needs and professional roles (Winter & Davidson, 2019). In the context of the KJP, tagging sensitive data is part of the system design, which must differentiate access levels between doctors, nurses, administrative staff, and policymakers. This is why the integration of the KJP–SATUSEHAT system is not only about technical interoperability, but also about the logical separation of data structures to prevent automation that erodes medical confidentiality.

Therefore, the system needs to be equipped with role-based access control (RBAC). The RBAC principle states that access is granted based on role and function, not formal position or bureaucratic proximity. Research in information security management shows that RBAC is the most effective mechanism for preventing least privilege access and minimizing the risk of internal abuse (Ugbaja et al., 2023). Within the KJP ecosystem, RBAC must be implemented granularly—for example, registration officers may only access basic identity information, not medical history; while specialist doctors may access complete medical records but not social administration information. This deepening of access granularity is a prerequisite for preventing data breaches arising from privilege escalation, which is frequently found in digital health systems in various countries.

However, RBAC will not work without robust oversight instruments. Therefore, privacy policy reform also demands strengthening audit logs and user behavior analytics. With an automatic recording system for every user action—from logins and file access, data modifications, to attempted unauthorized access—KJP can perform early detection of anomalies that indicate potential data leaks or misuse (Mansur & Zaman, 2023). Literature shows that comprehensive audit logs are the foundation of accountability in the digital health sector because they enable organizations to demonstrate compliance and trace incidents in a forensic-ready manner (Rindfleisch, 2000). Strengthening this monitoring is increasingly crucial in the era of big data, as the volume and velocity of data flows have surpassed the capabilities of manual supervision.

Transforming privacy policies is not only a technical-legal issue, but also touches on the human dimension, particularly the challenges of human resources, training, and a new work culture. The PDP Law shifts the work paradigm from "as long as the system works" to "safe, compliant, and documented." Many healthcare workers and administrative staff are not yet accustomed to thinking in a privacy-by-design framework, so reform requires ongoing training and a shift in organizational culture (van Rest et al., 2014). As Kotter (2012) noted, organizational change can only be successful if it involves building a sense of urgency, a leadership coalition, and the internalization of new norms (Kotter, 1996). Without cultural change, even the most sophisticated data security technology will be ineffective in preventing the risk of human error.

These challenges are compounded by regulatory deadline pressures, particularly after 2023, when the PDP Law will be gradually implemented. Many healthcare institutions, including KJP providers, are forced to accelerate transformations that are not always accompanied by technical and financial readiness. Time pressures create high administrative burdens—from developing new privacy policies and testing security systems to establishing Data Protection Officer (DPO) teams to mapping complex data flows. Public policy studies show that rapid compliance with new regulations often results in compliance fatigue and increased operational costs (Lambert, 2016).

However, in the long term, privacy policy reform has a positive impact on trust, compliance, and accountability. Clarity of procedures, transparency in data management, and stronger protection of sensitive information strengthen public trust in the health system. In line with organizational legitimacy theory, a system that complies with regulations and protects the rights of data subjects will gain greater social legitimacy, ultimately improving the quality of services and the effectiveness of public health programs (Suchman, 1995). Therefore, the KJP privacy policy reform is not merely an administrative adjustment, but part of the country's structural transformation in building a safe, ethical, and accountable digital health ecosystem.

Theoretical Analysis: Institutionalism, Systems Theory, Data Governance, and Change Management

From an institutional theory perspective, the adoption of EMR by healthcare facilities like KJP can be understood as a form of coercive isomorphism (Amenta & Ramsey, 2010). Dimaggio and Powell state that organizations tend to standardize practices to gain legitimacy when facing pressure from external institutions such as the government, regulators, or professional authorities (Dobbin, 2021). Minister of Health Regulation No. 24/2022 is an explicit instrument of coercive pressure: it sets national deadlines, technical standards, and reporting mechanisms that all healthcare facilities must comply with. This coercive pressure not only encourages the adoption of new technologies but also forces organizations to adapt their structures, processes, and work cultures to be consistent with regulatory expectations. In this context, KJP adjusted internal policies, changed record-keeping processes, and invested additional resources not solely out of economic incentives, but out of a need to gain institutional legitimacy under Indonesia's digital health governance (Lustig et al., 2014).

Digital health regulation also serves as a source of organizational legitimacy. In the healthcare sector, legitimacy stems not only from service quality but also from compliance with state-established legal and technical standards. When a healthcare facility can demonstrate that its digital system is integrated with official state platforms, such as SATUSEHAT, it gains legitimacy through what Suchman (1995) calls regulatory legitimacy. This legitimacy is crucial not only for the healthcare facility's reputation but also for operational continuity amidst increasing state control over health data governance (Suchman, 1995). Thus, implementing EMR is not merely a technical process but also an organizational strategy to maintain its position within an increasingly standardized national healthcare ecosystem.

Meanwhile, systems theory provides a complementary perspective to understanding SATUSEHAT integration. Systems theory, as formulated by Bertalanffy (1968), views organizations as part of a larger system, where effectiveness is only achieved when subsystems interact harmoniously (Von Bertalanffy, 1968). In the context of Indonesian digital health, interoperability is a key principle that enables clinical, administrative, laboratory, pharmacy, and referral system subsystems to be connected through SATUSEHAT. Regulations mandating the use of HL7 FHIR, ICD-10, and LOINC standards reflect the application of systemic logic: the country seeks to unify various, previously fragmented health information systems into an integrated national ecosystem. Without interoperability, patient data would be locked within silos of individual health facilities, leading to information discontinuity that could compromise patient safety and service quality. Therefore, SATUSEHAT integration is a manifestation of efforts to build system coherence within the Indonesian health ecosystem (Kellermann et al., 2013).

The integration of healthcare facility subsystems through SATUSEHAT also reflects a top-down system integration process, with the state acting as the primary architect. This national platform not only connects healthcare facilities but also standardizes how they manage data, code diagnoses, present patient histories, and communicate with referral systems. From a systems theory perspective, SATUSEHAT functions as a central orchestrator, ensuring that the entire ecosystem operates as a coherent entity, despite being comprised of thousands of organizations with varying levels of technological capacity (Hurmelinna-Laukkanen & Nätti, 2018). Thus, this integration is not simply a data transfer, but rather a reconstruction of the health communication structure at the national level.

Another highly relevant aspect is data governance theory, which highlights how the state acts as the manager, guardian, and primary stakeholder of health data. In the era of big data, health data has become a strategic asset for

both clinical decision-making and public policy. The state, through the PDP Law, Minister of Health Regulation 24/2022, and the SATUSEHAT policy, plays the role of data steward, an entity responsible for ensuring that personal data—especially sensitive health data—is managed according to the principles of privacy, security, and fairness (Khatri & Brown, 2010). This role is increasingly important as the digital transformation of health care not only expands the scope of data collection but also increases the risk of privacy violations and data misuse.

Health data ethics has become a central issue amid the growth of data-driven health governance. The availability of large amounts of data enables countries to conduct real-time epidemiological monitoring, quality control of services, and evidence-based resource allocation. However, data-driven governance models also carry risks such as surveillance creep, excessive data collection, unequal data access, and the potential commercialization of health information. Zuboff (2019) warns that the public needs to be wary of surveillance capitalism practices that exploit personal data as a commodity (Zuboff, 2019). In the health context, these risks are even greater because medical data is highly sensitive. Therefore, the implementation of SATUSEHAT must always be considered within a data ethics framework that balances the public value of health data with individual privacy rights.

Meanwhile, from an organizational change management perspective, the implementation of the SATUSEHAT Mandate reflects the dynamics of rapid change triggered by legal mandates. Kotter's (1996) eight-step model is highly relevant to understanding the changes at KJP (Kotter, 1996). First, the December 2023 deadline created a strong sense of urgency. Second, KJP formed a small team that served as a guiding coalition to manage the digitalization process. Third, the clinic developed a vision for change, including a full transition to RME and integration with SATUSEHAT. Fourth, this vision was communicated through internal training and meetings. Fifth, technical barriers such as server capacity and staff training were addressed through work restructuring and technical support. Sixth, the success of interoperability testing became a short-term win that boosted organizational confidence (Teramoto et al., 2024). Seventh, the digitalization process was strengthened through new internal policies on data privacy and security. Eighth, these changes were institutionalized in a new, all-digital work culture.

From Kotter's perspective, the changes in the KJP demonstrate how regulatory mandates can accelerate digital transformation processes that might not otherwise occur organically (Kotter, 1996). This means that digital health regulations are not merely instruments of coercion, but also catalysts for organizational change. Thus, the connection between regulation, organizational capacity, and technology is key to understanding the transformation of Indonesia's health sector.

Synthetically, the relationship between law, technology, and organizations forms the overall framework for national digital health transformation. Law creates the rules of the game, technology provides the infrastructure and standards, and organizations interpret and implement these rules in practice (de Vaujany et al., 2018). These three elements form a mutually influencing ecosystem: regulations establish interoperability standards; technology enables the implementation of these standards; and organizations like KJP translate these standards into operational practices. When these three elements work in harmony, digital health transformation can be effective and result in improved service quality, efficiency, and accountability.

Thus, the RME–SATUSEHAT integration cannot be viewed as a mere technical policy, but rather as an institutional restructuring process driven by regulations, supported by systemic technology, governed by data governance principles, and realized through organizational-level change management. This transformation is the foundation for building a more resilient, responsive, and data-driven health system in Indonesia (Compton & Benedetti, 2010).

CONCLUSION

This study answers the main question of how the Indonesian legal framework—including the Health Law, Ministerial Regulation No. 24/2022, and the 2022 PDP Law—is implemented in the practice of integrating Electronic Medical Records (EMR) with the SATUSEHAT system at the Padjadjaran Network Clinic (KJP). The research findings indicate that KJP was ultimately able to meet regulatory demands through digital infrastructure modernization, strengthening data governance, gradual training, and interoperability testing based on the HL7 FHIR standard. However, this success was achieved through a long and friction-filled adaptation process, ranging from staff resistance, the administrative burden of EMRO registration, regulatory gaps, and weak privacy literacy at the patient level.

From a theoretical perspective, this study emphasizes the relevance of institutional theory, systems theory, data governance theory, and change management in explaining the dynamics of digital health transformation in

Indonesia: regulations function as coercive pressure, the SATUSEHAT ecosystem as a systemic orchestrator, the state as a data steward, and organizations as adaptive agents continuously negotiating their identities and practices. Practically, this study emphasizes the importance of regulatory harmonization, improved consent mechanisms, enhanced patient education, and more proportional policy support for health facilities with limited capacity. The limitations of this study lie in the scope of a single case study and limited access to certain internal documents, so generalizations should be made with caution. For further research, comparative studies across health facilities, analysis of long-term impacts on service quality, and exploration of alternative governance models that are more adaptive to the evolving digital ecosystem are needed.

REFERENCES

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, *23*(5–6), 839–859. https://doi.org/10.1007/s00779-017-1104-3

Amenta, E., & Ramsey, K. M. (2010). *Institutional Theory* (pp. 15–39). https://doi.org/10.1007/978-0-387-68930-2_2

Arabi, Y. M., Al Ghamdi, A. A., Al-Moamary, M., Al Mutrafy, A., AlHazme, R. H., & Al Knawy, B. A. (2022). Electronic medical record implementation in a large healthcare system from a leadership perspective. *BMC Medical Informatics and Decision Making*, *22*(1), 66. https://doi.org/10.1186/s12911-022-01801-0

Asyfia, A., Zaid, 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

Bender, D., & Sartipi, K. (2013). HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. *Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems*, 326–331. https://doi.org/10.1109/CBMS.2013.6627810

Benneh Mensah, G., & Dutta, P. K. (2024). Evaluating if Ghana's Health Institutions and Facilities Act 2011 (Act 829) Sufficiently Addresses Medical Negligence Risks from Integration of Artificial Intelligence Systems. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2024*, 35–41. https://doi.org/10.58496/MJAIH/2024/006

Compton, J. R., & Benedetti, P. (2010). LABOUR, NEW MEDIA AND THE INSTITUTIONAL RESTRUCTURING OF JOURNALISM. *Journalism Studies*, *11*(4), 487–499. https://doi.org/10.1080/14616701003638350

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches, Fifth Edition*. SAGE Publications Asia-Pacific Pte. Ltd.

Custers, B., Sears, A. M., Dechesne, F., Georgieva, I., Tani, T., & van der Hof, S. (2019). *EU Personal Data Protection in Policy and Practice* (Vol. 29). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-282-8

Darnela, L., & Rusdiana, E. (2025). Public Legal Awareness and the Effectiveness of Indonesia's Personal Data Protection Law: Bridging Normative Framework and Privacy Paradox. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, *14*(1), 1–28. https://doi.org/10.14421/2gg2rp29

de Vaujany, F.-X., Fomin, V. V., Haefliger, S., & Lyytinen, K. (2018). Rules, Practices, and Information Technology: A Trifecta of Organizational Regulation. *Information Systems Research*, *29*(3), 755–773. https://doi.org/10.1287/isre.2017.0771

Dobbin, F. (2021). *The New Economic Sociology : A Reader*. Princeton University Press CN - HB.

Engle, C. R., van Senten, J., Clark, C., & Boldt, N. (2023). Has the Regulatory Compliance Burden Reduced Competitiveness of the U.S. Tilapia Industry? *Fishes*, *8*(3), 151. https://doi.org/10.3390/fishes8030151

Faisal, K. (2023). Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective. *Communication Law and Policy*, *28*(1), 67–97. https://doi.org/10.1080/10811680.2023.2180266

Fitri, R. D., Hilman, M., & Yazid, S. (2025). Improving password policy strategies: a government employee perspective. *Information & Computer Security*, *33*(4), 547–572. https://doi.org/10.1108/ICS-12-2024-0335

Forgó, N., Hänold, S., & Schütze, B. (2017). *The Principle of Purpose Limitation and Big Data* (pp. 17–42). https://doi.org/10.1007/978-981-10-5038-1_2

Goswami, S. S., & Mondal, S. (2025). Data Security and Privacy Concerns in Digitized Medical Services: Implications for Malpractice Risk Management. *Spectrum of Decision Making and Applications*, *3*(1), 212–242. https://doi.org/10.31181/sdmap31202643

Hariharan, S., Jonnalagadda, R., Walrond, E., & Moseley, H. (2006). Knowledge, attitudes and practice of healthcare ethics and law among doctors and nurses in Barbados. *BMC Medical Ethics*, *7*(1), 7. https://doi.org/10.1186/1472-6939-7-7

Helén, I., & Tarkkala, H. (2024). Adjusting expectations actionable: Personalised treatment plan in anticipation of data-driven healthcare. *Big Data & Society*, *11*(4). https://doi.org/10.1177/20539517241285384

Hulkower, R., Penn, M., & Schmit, C. (2020). *Privacy and Confidentiality of Public Health Information* (pp. 147–166). https://doi.org/10.1007/978-3-030-41215-9_9

Hurmelinna-Laukkanen, P., & Nätti, S. (2018). Orchestrator types, roles and capabilities – A framework for innovation networks. *Industrial Marketing Management*, *74*, 65–78. https://doi.org/10.1016/j.indmarman.2017.09.020

Isibor, E. (2024). *Regulation of Healthcare Data Security: Legal Obligations in A Digital Age*. https://doi.org/10.2139/ssrn.4957244

Jimenez, G., Spinazze, P., Matchar, D., Koh Choon Huat, G., van der Kleij, R. M. J. J., Chavannes, N. H., & Car, J. (2020). Digital health competencies for primary healthcare professionals: A scoping review. *International Journal of Medical Informatics*, *143*, 104260. https://doi.org/10.1016/j.ijmedinf.2020.104260

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. https://doi.org/10.14710/lenpust.v11i1.70518

Kellermann, A. L., Saultz, J. W., Mehrotra, A., Jones, S. S., & Dalal, S. (2013). Primary Care Technicians: A Solution To The Primary Care Workforce Gap. *Health Affairs*, *32*(11), 1893–1898. https://doi.org/10.1377/hlthaff.2013.0481

Khanna, V., & Kotwal, A. (2025). Examining the significance of the digital personal data protection act, 2023 in the context of the healthcare industry: a comprehensive analysis. *Discover Public Health*, *22*(1), 381. https://doi.org/10.1186/s12982-025-00757-6

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148–152. https://doi.org/10.1145/1629175.1629210

Kotter, J. P. (1996). *Leading Change*. Harvard Business Review Press.

Kovan, A. (2025). Digital Fatigue within the Family: Psychosocial Reflections of Constant Connectedness. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, *27*(Aile Özel Sayısı), 333–350. https://doi.org/10.32709/akusosbil.1722337

Kulp, L., Sarcevic, A., Zheng, Y., Cheng, M., Alberto, E., & Burd, R. (2020). Checklist Design Reconsidered: Understanding Checklist Compliance and Timing of Interactions. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376853

Lambert, P. (2016). *The Data Protection Officer*. Auerbach Publications. https://doi.org/10.1201/9781315396743

Lestari, E., & Rasji, R. (2024). Legal Study On Personal Data Protection Based On Indonesian Legislation. *Awang Long Law Review*, *6*(2), 471–477. https://doi.org/10.56301/awl.v6i2.1206

López, O. (2020). *Ensuring the Integrity of Electronic Health Records*. Productivity Press. https://doi.org/10.4324/9781003105695

Lubello, V., & Vedaschi, A. (2015). Data Retention and its Implications for the Fundamental Right to Privacy. *Tilburg Law Review*, *20*(1), 14–34. https://doi.org/10.1163/22112596-02001005

Lustig, N., Pessino, C., & Scott, J. (2014). The Impact of Taxes and Social Spending on Inequality and Poverty in Argentina, Bolivia, Brazil, Mexico, Peru, and Uruguay. *Public Finance Review*, *42*(3), 287–303. https://doi.org/10.1177/1091142113506931

Lyu, G. (2025). Data-driven decision making in patient management: a systematic review. *BMC Medical Informatics and Decision Making*, *25*(1), 239. https://doi.org/10.1186/s12911-025-03072-x

Mahmoudi, E., Kamdar, N., Kim, N., Gonzales, G., Singh, K., & Waljee, A. K. (2020). Use of electronic medical records in development and validation of risk prediction models of hospital readmission: systematic review. *BMJ*, m958. https://doi.org/10.1136/bmj.m958

Mansur, A. Al, & Zaman, T. (2023). User Behavior Analytics in Advanced Persistent Threats: A Comprehensive Review of Detection and Mitigation Strategies. *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, 1–6. https://doi.org/10.1109/ISAS60782.2023.10391553

Muinga, N., Magare, S., Monda, J., English, M., Fraser, H., Powell, J., & Paton, C. (2020). Digital health Systems in Kenyan Public Hospitals: a mixed-methods survey. *BMC Medical Informatics and Decision Making*, *20*(1), 2. https://doi.org/10.1186/s12911-019-1005-7

Naili, Y. T., Afrilies, M. H., Garunja, E., & Purwono, P. (2024). Protection of patient data privacy on IoT devices for healthcare in the era of smart cities: a health law perspective. *Jurnal Hukum Novelty*, *15*(1), 87. https://doi.org/10.26555/novelty.v15i1.a28457

NE Varuhas, J. (2023). Mapping doctrinal methods. In *Researching Public Law in Common Law Systems* (pp. 70–103). Edward Elgar Publishing. https://doi.org/10.4337/9781789904383.00009

Nurmaidah, N., Kustiningsih, N., & Rahayu, S. (2024). Change management strategy in the implementation of electronic medical record system in the era of digital transformation: Case study at Rahman Rahim Hospital. *Gema Wiralodra*, *15*(1), 228–238. https://doi.org/10.31943/gw.v15i1.656

Osborn, A. G., Louis, D. N., Poussaint, T. Y., Linscott, L. L., & Salzman, K. L. (2022). The 2021 World Health Organization Classification of Tumors of the Central Nervous System: What Neuroradiologists Need to Know. *American Journal of Neuroradiology*, *43*(7), 928–937. https://doi.org/10.3174/ajnr.A7462

Pallocci, M., Treglia, M., Passalacqua, P., Tittarelli, R., Zanovello, C., De Luca, L., Caparrelli, V., De Luna, V., Cisterna, A. M., Quintavalle, G., & Marsella, L. T. (2023). Informed Consent: Legal Obligation or Cornerstone of the Care Relationship? *International Journal of Environmental Research and Public Health*, *20*(3), 2118. https://doi.org/10.3390/ijerph20032118

Prang, K.-H., Canaway, R., Bismark, M., Dunt, D., & Kelaher, M. (2018). The use of public performance reporting by general practitioners: a study of perceptions and referral behaviours. *BMC Family Practice*, *19*(1), 29. https://doi.org/10.1186/s12875-018-0719-4

Rindfleisch, A. (2000). Organizational Trust and Interfirm Cooperation: An Examination of Horizontal Versus Vertical Alliances. *Marketing Letters*, *11*(1), 81–95. https://doi.org/10.1023/A:1008107011529

Saeed, S. A., & Masters, R. M. (2021). Disparities in Health Care and the Digital Divide. *Current Psychiatry Reports*, *23*(9), 61. https://doi.org/10.1007/s11920-021-01274-4

Sarabdeen, J., & Mohamed Ishak, M. M. (2025). A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR). *International Journal of Law and Management*, *67*(1), 99–119. https://doi.org/10.1108/IJLMA-01-2024-0025

Schmidt, J., Schutte, N. M., Buttigieg, S., Novillo-Ortiz, D., Sutherland, E., Anderson, M., de Witte, B., Peolsson, M., Unim, B., Pavlova, M., Stern, A. D., Mossialos, E., & van Kessel, R. (2024). Mapping the regulatory landscape for artificial intelligence in health within the European Union. *Npj Digital Medicine*, *7*(1), 229. https://doi.org/10.1038/s41746-024-01221-6

Setyani, S. A., & Mahendro, P. K. (2025). Application of Heuristic Algorithm in Medical Informatics System for Patient Data Management in Southeast Asia. *Indonesian Journal of Electronics, Electromedical Engineering, and Medical Informatics*, *7*(1), 64–76. https://doi.org/10.35882/7ygpx615

Sijabat, H. H., & Tridewiyanti, K. (2022). Feminism criticism of abortion provisions of rape victims according to law number 36 the year 2009 on health. *Linguistics and Culture Review*, *6*, 205–215. https://doi.org/10.21744/lingcure.v6nS5.2139

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management Review*, *20*(3), 571–610. https://doi.org/10.5465/amr.1995.9508080331

Sugiarti, I. (2020). Legal Protection of Patient Rights to Completeness and Confidentiality in Management of Medical Record Documents. *The Proceedings of the 2nd Bakti Tunas Husada-Health Science International Conference (BTH-HSIC 2019)*. https://doi.org/10.2991/ahsr.k.200523.045

Teramoto, A., Sakamaki, K., Shoji, S., & Uemura, K. (2024). Win ratio analysis of short-term clinical outcomes of focal therapy and robot-assisted radical prostatectomy for the patients with localized prostate cancer. *Scientific Reports*, *14*(1), 17019. https://doi.org/10.1038/s41598-024-67592-8

Tilaar, T. S., & Sewu, P. L. S. (2023). Review of Electronic Medical Records in Indonesia and its Developments Based on Legal Regulations in Indonesia and its Harmonization with Electronic Health Records (Manual for Developing Countries). *Daengku: Journal of Humanities and Social Sciences Innovation*, *3*(3), 422–430. https://doi.org/10.35877/454RI.daengku1662

Tourani, R., Misra, S., Mick, T., & Panwar, G. (2018). Security, Privacy, and Access Control in Information-Centric Networking: A Survey. *IEEE Communications Surveys & Tutorials*, *20*(1), 566–600. https://doi.org/10.1109/COMST.2017.2749508

Ugbaja, U. S., Nwabekee, U. S., Owobu, W. O., & Abieba, O. A. (2023). Conceptual Framework for Role-Based Network Access Management to Minimize Unauthorized Data Exposure Across IT Environments. *International Journal of Social Science Exceptional Research*, *2*(1), 211–221. https://doi.org/10.54660/IJSSER.2023.2.1.211-221

van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2014). *Designing Privacy-by-Design* (pp. 55–72). https://doi.org/10.1007/978-3-642-54069-1_4

VanGestel, R., & Micklitz, H.-W. (2011). Revitalizing Doctrinal Legal Research in Europe: What About Methodology? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1824237

Vedder, A., & Spajić, D. (2023). Moral autonomy of patients and legal barriers to a possible duty of health related data sharing. *Ethics and Information Technology*, *25*(1), 23. https://doi.org/10.1007/s10676-023-09697-8

Von Bertalanffy, L. (1968). General system theory. *New York*, *41973*(1968), 40.

Webster, A., & Gardner, J. (2019). Aligning technology and institutional readiness: the adoption of innovation. *Technology Analysis & Strategic Management*, *31*(10), 1229–1241. https://doi.org/10.1080/09537325.2019.1601694

Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *The Information Society*, *35*(1), 36–51. https://doi.org/10.1080/01972243.2018.1542648

Xiao, D., Song, C., Nakamura, N., & Nakayama, M. (2021). Development of an application concerning fast healthcare interoperability resources based on standardized structured medical information exchange version 2 data. *Computer Methods and Programs in Biomedicine*, *208*, 106232. https://doi.org/10.1016/j.cmpb.2021.106232

Yeng, P. K., Fauzi, M. A., Sun, L., & Yang, B. (2022). Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development. *JMIR Human Factors*, *9*(2), e30050. https://doi.org/10.2196/30050

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (http://creativecommons.org/licenses/by-sa/4.0/).