Architecture
Image Studies

Vol.6, Issue 4, pp.669-679, 2025
DOI: https://doi.org/10.62754/ais.v6i4.667

https://journals.ap2.pt/index.php/ais/index

Analysis of the Policy on the Misuse of Medical Record Data by Health Care Facilities

Diaz Alifarizki Zuvarcan[1], Arief Budiono[2], Wardah Yuspin[3], Valisher Sapayev[4], Normuratov Aktam[5]

Abstract

Introduction: This study examines the legal aspects of medical record data misuse by healthcare facilities in Indonesia, emphasizing its ethical, legal, and systemic implications. Medical records are crucial to prevent data privacy violations, unauthorized access, and commercial exploitation. Methodology: Using the normative juridical research method, this qualitative study analyzes the legal framework, including Law Number 17 of 2023 on Health, the Personal Data Protection Law, and other relevant legislation, complemented by scientific literature and case studies. The research findings reveal that medical record misuse often occurs through unauthorized access, false claims, data manipulation, and illegal data sharing with third parties, reflecting gaps in law enforcement and weak institutional governance. This study highlights the strong link between medical record misuse and healthcare fraud, demonstrating how systemic pressures and inadequate oversight encourage unethical practices. This study recommends strengthening regulatory integration, improving cybersecurity infrastructure, implementing stricter sanctions, and increasing ethical awareness among healthcare professionals. This research contributes to the health law discourse by offering actionable legal and policy recommendations while emphasizing the need for a cultural shift toward transparency and data management. Future studies should incorporate empirical fieldwork and explore advanced digital security innovations to address emerging challenges.

Keywords: *Fraud, Health Law, Health Service Facilities, Medical Records.*

Introduction

Medical records serve as a critical component of healthcare management, containing comprehensive patient information, including diagnoses, treatment history, medications, and other sensitive data. Medical records not only facilitate effective patient care but also serve as legal documents that protect both patients and healthcare providers in the event of a medical dispute. Given the highly confidential nature of medical records, all healthcare providers have the fundamental ethical and legal obligation to maintain their security and integrity. However, the increasing adoption of digital medical record systems, along with advances in healthcare information technology, has raised concerns about data privacy, security breaches, and potential misuse by healthcare facilities (Tilaar & Sewu, 2023).

In Indonesia, various laws and policies regulate medical record protection and management, including Law No. 17 of 2023 on Health, Government Regulation No. 71 of 2019 on Electronic Systems and Transactions, and Minister of Health Regulation No. 269/MENKES/PER/III/2008 on Medical Records. These legal frameworks emphasize that patient medical information must be kept confidential and may only be accessed by authorized personnel for medical purposes. Despite these regulations, there have been reports of numerous cases of unauthorized access, illegal distribution, and inappropriate use of medical records. These incidents raise significant concerns about the effectiveness

[1] Department of Law, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia, Emails: alifarizki1@gmail.com
[2] Department of Law, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia, Email: ab368@ums.ac.id, (Corresponding Author)
[3] Department of Law, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia, Email: wy204@ums.ac.id
[4] General Professional Science Department, Mamun University, Uzbekistan, Email: sapayev.vali.2017@gmail.com
[5] Tashkent State University of Law, Uzbekistan, Email: aktamnurmurato@gmail.com5

of existing legal protection and healthcare providers' level of compliance (Larasati, Fardiansyah, Saketi, & Dewiarti, 2024).

One of the most concerning forms of medical record misuse is the unauthorized sharing of patient data for commercial purposes. Some healthcare facilities have been found to sell or disclose patient information to third parties, such as pharmaceutical companies, insurance companies, or marketing agencies, without these patients' consent. This practice not only violates patient privacy but also undermines the ethical principles of medical practice. Furthermore, medical record breaches have led to cases of identity theft, fraud, and discrimination, particularly when sensitive health information is used by employers or insurance companies to deny individuals certain rights or benefits (Ramadianto, 2023).

A 2022 study by Marwiyah entitled "Analysis of Legal Review of Medical Information Release to Ensure the Confidentiality of Patient Identity", which was published in the Awang Long Law Review, examines the legal aspects of medical information disclosure to ensure patient confidentiality. The study concluded that healthcare facilities have a legal obligation to protect medical information contained in medical records from losses, damages, falsification, and unauthorized access (Marwiyah, 2022).

Next, a 2024 study by Larasati et al., entitled "The Ethical and Legal Aspects of Health Policy on Electronic Medical Records in Indonesia", was published in the Cepalo Journal. It examined the ethical and legal aspects of electronic medical records (EMR) policies in Indonesia. The study concluded that there are challenges to the implementation of EMR in terms of data security, healthcare worker readiness, and uneven internet infrastructure across Indonesia. Although the Regulation of the Minister of Health No. 24 of 2022 regulates the legality of EMR, the risk of data breaches remains a major concern, necessitating stricter security measures to protect patient privacy. Furthermore, the integration of EMR with the Ministry of Health's systems raises concerns regarding the potential for unauthorized access and misuse of patient data (Larasati et al., 2024).

A study conducted by Anwar et al. in 2025 entitled "Juridical Analysis of the Misuse of Electronic Medical Records in the Perspective of the Electronic Information and Transaction Law" concluded that electronic medical records are vulnerable to misuse, particularly in the form of unauthorized access and leakage of patient data. Law No. 1 of 2024 stipulates that electronic information can be used as evidence in court in the event of illegal distribution of medical data, while Law No. 27 of 2022 emphasizes healthcare providers' obligation to protect patients' personal data. Therefore, there is a need for strategic steps, such as improving the digital security system, implementing strict policies on data access, and educating healthcare workers about the ethics and laws of patient data protection (Anwar, Tambun, & Jaeni, 2025).

Another significant issue is the lack of robust enforcement and oversight mechanisms to ensure compliance with laws on medical record protection. Many healthcare institutions, particularly smaller clinics and regional hospitals, may lack the cybersecurity infrastructure or legal awareness necessary to prevent data breaches. In some cases, hospital staff may even be complicit in unauthorized access to medical records due to weak internal controls or inadequate legal consequences for breaches. This gap highlights the need for a stronger regulatory framework that not only establishes clear guidelines but also ensures that violations are subject to strict penalties (Anwar et al., 2025).

Given these challenges, this study aims to conduct a legal analysis of the misuse of medical records in healthcare facilities, examining existing legal provisions and their practical enforcement. By reviewing relevant case studies and legal precedents, this study seeks to identify systemic weaknesses in the current regulatory framework and propose policy recommendations to strengthen data protection mechanisms. Furthermore, this study will explore the ethical implications of the misuse of medical records and assess the role of healthcare institutions in protecting patient confidentiality (Lukitasari, Huda, & Asmuni, 2023).

Ultimately, ensuring the security and appropriate use of medical records is crucial to maintaining public trust in the healthcare system. Without adequate legal protection and effective enforcement measures, the risk of data breaches and misuse will continue to threaten patient rights and medical ethics. This research aims to establish a clearer legal framework to increase accountability and strengthen the protection of medical record confidentiality in the Indonesian healthcare sector (Komalasari & Mustafa, 2024).

The problem formulation in this research is: What legal policies can be implemented to strengthen the protection of medical record data and prevent its misuse by health service facilities?

Methodology

The research methodology applied in this study is normative legal research, which emphasizes the analysis and interpretation of various legal documents, laws, literature, and existing legal concepts (Jiwanti & Soponyono, 2022). According to Soerjono Soekanto, normative legal research is legal research that focuses on the review and analysis of written laws, theories, concepts, and legal principles, using library materials or secondary data as the main source without conducting direct observations in the field (Benuf & Azhar, 2020).

In normative legal research, researchers collect and evaluate various legal sources, including statutes, regulations, court decisions, legal expert opinions, and relevant legal literature. The primary goal of this research is to understand and interpret legal standards, statutory requirements, and concepts related to the analyzed subject (Kelik Wardiono, 2019).

This study used a statute and library research approach to analyze legal issues related to the misuse of medical record data. The statute approach is a method to examine legal issues by directly referring to applicable laws and regulations as the primary legal basis. This is as explained by Soekanto, who stated that this approach is used to systematically understand the content of legal norms (Soekanto, 2012). Meanwhile, the library research approach was conducted by exploring secondary legal materials, such as legal literature, journal articles, and court decisions, to strengthen legal analysis and interpretation (Wiraguna, 2025). Through the combination of these two approaches, researchers can build a comprehensive and in-depth legal framework regarding the topic discussed, as well as produce a systematic, logical, and structured understanding of the law.

This research was conducted using data collection tools that include legislations (statue approach) and literature (library approach) to collect secondary data related to the research problem, by studying books, legal journal articles, research results, and statutory regulatory documents, such as: Law Number 17 of 2023 on Health, Law Number 1 of 2023 on the Criminal Code, Government Regulation No. 71 of 2019 on Electronic Systems and Transactions, Law Number 27 of 2022 on Personal Data Protection, Minister of Health Regulation Number 24 of 2022 on Medical Records, Minister of Health Regulation Number 20 of 2019 on the Provision of Telemedicine Services Between Health Service Facilities, and the Indonesian Medical Council Regulation Number 74 of 2020.

The data analysis in this study was conducted using the qualitative descriptive method based on the normative juridical method. The stages of data analysis in this study refer to legal analysis methods. First, data identification and classification were carried out, namely sorting and grouping data based on the type of legal source, such as from legislation, academic journals, or court decisions. Second, a normative analysis was conducted, where the authors analyzed regulations relevant to the misuse of medical record data and compared them with the principles of health law and personal data protection. Third, using the interpretation method, the legal interpretation was applied, such as grammatical interpretation (based on legal texts), systematic interpretation (connecting various related legal rules), and teleological interpretation (looking at the purpose of the law in protecting patient rights).

Results and Discussion

Inequality in Regulation and Implementation

On paper, the legal architecture for protecting medical records appears coherent. However, in practice, it is fragmented. National regulations mandate electronic medical records and connectivity to common platforms, but there is a gap between the regulations and routine compliance. Some provisions serve as general norms, while others are highly technical. Without a single, detailed guideline that translates broad mandates into operational steps for each facility class, hospitals and clinics interpret obligations differently, resulting in diverse practices across the country (Novianti & Bakhtiar, 2024).

Compliance is strongly correlated with resources and governance maturity. Large urban hospitals typically have dedicated IT teams, formal information security policies, and budgets for upgrades, while smaller clinics and rural facilities often lack these. This disparity manifests itself in basic controls, such as role-based access, password standards, and workstation security. It also manifests in more sophisticated requirements, such as separating production and test databases or conducting vulnerability scans, which can only be consistently met by providers with better resources. As a result, there are varying levels of patient data protection depending on where they seek care (Ratnawati & Iskandar, 2025). Another source of variability is integration with national platforms.

Facilities use a variety of MIS vendors and specialized systems, many of which outpace current interoperability and security expectations. Routine challenges include mapping legacy data to required formats, harmonizing patient identifiers, and ensuring stable API connections. When systems don't natively support required standards, providers rely on manual solutions or ad-hoc middleware, which creates security gaps and data quality issues (Roro, Satyoputri, & Sidi, 2024).

Technical safeguards are inconsistently implemented. Encryption at rest and in transit, hardened server configurations, and endpoint protection are common in tertiary hospitals but far from universal primary care settings. Network segmentation, firewalls configured with least privilege rules, and multifactor authentication are still in their infancy. Even when facilities have the right tools, default settings are often left unchanged, logs are not retained long enough to be useful, and alerts are not prioritized because no one is formally tasked with monitoring them (Azwar & Sirait, 2025).

Audit practices exhibit similar gaps. Many service providers limit audits to annual administrative checklists that focus on documentation rather than testing the effectiveness of controls. Few conduct genuine security assessments that include log reviews, access recertification, and breach simulations. When they occur, external audits tend to focus on financial claims rather than data protection, leaving technical risks under-assessed. In places without independent verification, self-declaration becomes the norm, while weaknesses stay unnoticed (Sadnyini, Christianto, Kurniawan, & Jayantara, 2024).

Organizational structures exacerbate the problem. Few facilities have designated data protection leaders or information security officers with the authority to enforce policies across clinical and administrative units. Without clear ownership, tasks such as maintaining access matrices, reviewing third-party contracts, or approving data sharing for research fall across departments. Committees exist on paper but meet irregularly, and incident response plans exist but remain untested (Rahayu, 2025).

Third-party risk management is also uneven. Telemedicine services, laboratory partners, cloud hosting, and billing platforms all process sensitive health data, but contracts do not always specify security requirements, breach notification periods, or audit rights. If data processing agreements are absent or unclear, accountability becomes diffuse, and post-incident remediation is slow and controversial. Facilities with greater bargaining power can demand stricter requirements; smaller providers often accept vendor templates that prioritize functionality over protection (Dalimunthe & Simarmata, 2021).

Daily clinical workflows present further variability. Some facilities restrict access to the “minimum necessary” data and periodically review user privileges; others grant broad access to avoid delays in care. In the latter, staff sometimes export or print large record sets for convenience, store them on personal devices, or share screenshots via consumer messaging apps when the system is slow. These habits arise from operational pressures but erode the protections intended by the legal framework (Roro et al., 2024).

Next, breach detection and reporting illustrate the maturity gap. Facilities with security information and event management (SIEM) tools, centralized logging, and well-trained escalation paths can detect anomalous access within hours. Meanwhile, others rely on ad-hoc discoveries, often stemming from patient complaints or IT outages, after which evidence is incomplete and notification timelines unclear. Without standard metrics for “what to report, to whom, and when,” similar incidents are handled differently across institutions (Kurniawan, Hehanussa, Setiawan, Susilowati, & Helfisar, 2024).

Due to inconsistent rollouts, data quality and interoperability are also compromised. If coding systems and master patient indexes are implemented correctly, then information flows securely and accurately. If not, record duplication, outcome misattribution, and transmission failures are common. In addition to privacy risks, these technical inconsistencies create clinical risks, thus undermining the broader policy goal of integrated, patient-centered care (Novianti & Bakhtiar, 2024).

The enforcement environment is perceived as varied. Some jurisdictions conduct active inspections and issue corrective action plans, while others emphasize guidance and education with limited follow-up. Without visible and proportionate sanctions for organizational failures, not just individual misconduct, leaders may neglect investments in security and governance. This perception exacerbates the implementation gap: those who act early continue to improve performance, while those who lag behind delay necessary improvements (Sadnyini et al., 2024).

Lack of Legal Coverage for Medical Personnel

Legal outreach in healthcare is often viewed as a compliance checkbox, rather than an ongoing professional obligation. Policies exist, but they are rarely translated into daily practices at the patients' treatment rooms, at the registration desk, or in the server room. When rules are enforced without a practical link to clinical workflows, staff revert to informal norms and time-saving shortcuts. The result is a wide gap between what the law expects and what teams actually do when caring for patients or processing claims (Widjaja, 2025).

Many physicians still view electronic medical records as purely clinical instruments, rather than legal documents that are subject to strict confidentiality obligations. This mindset leads to a permissive attitude toward "quick glances" at charts, widely sharing screenshots, or downloading data to personal devices to expedite care. In busy situations, the distinction between what is clinically beneficial and what is legally permissible becomes blurred. Without clear reminders and simple work tools, the "minimum necessary" principle is remembered in theory but forgotten in practice (Azwar & Sirait, 2025).

Knowledge gaps aren't limited to physicians. Nurses, pharmacists, medical records officers, billing staff, IT support, and security officers each handle patient data differently. If outreach targets only physicians, many risks remain unaddressed. For example, ward staff may be unaware that reusing generic logins can weaken traceability, or that printing census lists for convenience creates an unmanageable paperwork trail. Effective outreach requires mapping roles based on specific data handling risks and tailoring messaging (Roro et al., 2024).

One-off seminars rarely change behavior as staff attend orientation, sign forms, and move on. Months later, policies have been updated, new features have been added to the system, and third-party platforms have been integrated, but the initial training has not caught up. Sustainable programs prioritize short, repetitive microlearning sessions, scenario-based case studies, and brief refreshers tied to high-stakes moments, such as rotations, promotions, or system upgrades. Repetition and relevance keep the rules in place.

Legal language itself is a barrier. Regulations use abstract terms that are difficult to apply in real life. Concepts like informed consent, data minimization, purpose limitation, retention, and legal basis feel distant from reality unless translated into concrete dos and don'ts for common tasks: ordering labs for the wrong patient, forwarding discharge summaries, using messaging apps, or accessing coworkers' and families' medical records. Outreach must transform dense clauses into simple, role-specific checklists and decisions.

Operational pressures exacerbate the problem. When the system is slow, staff take screenshots of results and share them informally; when a patient is unstable, "break the glass" access becomes a routine and ordinary event. Without limitations, emergency assistance becomes everyday practice. Outreach needs to integrate education with system design: clear directions before "breaking the glass", automatic flagging for unusual access, and post-event reviews that are supportive rather than punitive.

The rotation of students and trainees adds another layer of risk. They require extensive exposure to learn, but broad access expands the attack surface. If outreach does not include pre-rotation briefings, temporary access profiles, and stringent end-of-rotation revocations, credentials will be compromised, and audit trails will be eroded.

Cultural dynamics are also important. In hierarchical environments, junior staff may hesitate to challenge questionable data requests from seniors or external parties. Outreach efforts should normalize "polite refusals" and provide written phrases to deflect inappropriate requests. Leaders need to publicly model such behavior, acknowledging when access is denied and praising staff who maintain privacy under pressure.

When people fear blame, incident reporting becomes difficult. Staff hide near-miss incidents, delete local files, or delay reporting to "fix it first." A just culture approach distinguishes between human error, risky behavior, and reckless behavior, each of which is combined with a proportionate response. Outreach must clearly explain this framework so that people feel safe reporting quickly, which is crucial for timely control and notification.

In internal training, relationships with third parties are often overlooked. Telemedicine providers, laboratories, cloud providers, and billing partners process the same sensitive data but may follow different guidelines. Through orientation briefings, shared minimum standards, and simple checklists

outlined in contracts, outreach should extend beyond the hospital. When vendors understand a facility's expectations from the outset, fewer conflicts arise after an incident (Novianti & Bakhtiar, 2024).

Measurement is often superficial. Online learning completion rates are tracked, but actual competency is not. Outreach should include brief knowledge checks, simulated phishing or subterfuge attempts, and targeted retraining for teams that show recurring gaps. Reviewing access logs can identify departments with unusual patterns, allowing for tailored microlearning rather than blanket reminders.

Language and accessibility are important considerations. Material written solely in legal or technical jargon will not reach busy clinicians. Outreach should use simple language, visuals, and real-life examples from the facility's own experiences. Translating core messages into local languages and adapting them to specific services—e.g., emergency, ICU, outpatient, and pharmacy—improves recall and relevance.

Time and place matter. Training scheduled during peak hours or added to lengthy meetings is often overlooked. Short, focused sessions embedded within existing touchpoints, such as shift handovers, morbidity and mortality meetings, quality rounds, or monthly grand rounds, reach more people with less resistance. Digital signage upon sign-in, laminated tips at workstations, and 60-second reminder videos on staff dashboards keep privacy a top priority.

Outreach should be linked to credentialing and re-credentialing. Granting or renewing access rights without verifying current competency creates a bias. Annual or semi-annual, streamlined, role-based, and scenario-driven recertification keeps standards relevant. Where possible, completion can be linked to assessments, clinical privileges, or eligibility for supervisory roles, signaling that privacy competency is a core professional skill.

Leaders set the tone. When executives and department heads attend the same training, reference privacy goals in performance reviews, and allocate budget and time for learning, staff recognize that this topic is non-negotiable. Conversely, when leaders ignore the "get things done" rule, the message falls flat. Outreach should include a leader's toolkit: talking points, a dashboard with simple metrics, and a clear escalation map for difficult calls.

Outreach works best when combined with user-friendly systems. If software implements role-based access by default, automatically logs every access, terminates sessions, and makes the appropriate path the fastest, education has a powerful ally. When systems work against workflow, training alone is insufficient. The long-term solution is a combined strategy: simplifying rules, embedding them in technology, reinforcing them with practical instruction, and measuring what matters (Widjaja, 2025).

Lack of Firmness in Institutional Sanctions

In cases of medical record misuse, current approaches to sanctions tend to be narrow and reactive. Most healthcare institutions treat violations as internal disciplinary matters, often resolved with written warnings, temporary suspensions, or reassignments of responsible staff. While these measures can improve behavior at the individual level, they rarely address the systemic weaknesses that led to the violations. By framing the problem as a single employee's failure, organizations avoid deeper accountability for structural gaps in training, supervision, or technology. This creates a cycle in which the same vulnerabilities remain unaddressed, increasing the likelihood of future violations (Sadnyini et al., 2024).

One major weakness is the lack of escalation of criminal or civil liability in the institution. In practice, healthcare facilities often rely on administrative remedies or "soft" sanctions, such as internal memos or managerial reprimands. Even when sensitive health data is leaked or misused, hospitals or clinics rarely face significant financial penalties, revocation of accreditation, or lawsuits. This leniency signals to institutions that the risks of non-compliance are negligible compared to the cost of investing in robust data protection systems. Over time, the lack of tangible consequences erodes incentives to improve security standards and fosters complacency.

This problem is exacerbated by an uneven enforcement landscape. Regulatory agencies may issue guidelines and conduct inspections, but follow-up after violations is inconsistent. Some facilities receive warnings or are required to submit corrective action plans, while others face no meaningful oversight at all. This inconsistency undermines the credibility of regulations and sends mixed messages

to healthcare organizations. Facilities that adhere to higher standards may find themselves shortchanged on their investment, while those that cut corners face only temporary scrutiny.

Another gap is the limited scope of sanctions. Most sanctions are administrative in nature, such as warning letters, staff rotations, or removal from certain responsibilities, without any material impact on the institution's operations. Fines commensurate with the severity of the violation, suspension of operating licenses, or requirements related to accreditation renewal are rare. Without strong, enforceable consequences, institutions lack a real sense of urgency to overhaul their systems, retrain their staff, or implement stronger safeguards. The lack of institutional accountability further shifts the burden onto individual workers, who may lack the resources, authority, or systemic knowledge to prevent violations on their own.

The lack of stringent sanctions has serious implications for public trust. Patients expect healthcare providers to safeguard their most sensitive information with the highest level of care. When breaches occur and institutions appear to get away with only a warning, patients can lose confidence in the security of digital health systems. This erosion of trust undermines national initiatives, such as the integration of electronic medical records, the expansion of telemedicine, and the digitization of health insurance claims, all of which depend on public acceptance and cooperation. If patients fear their data is unsafe, they may withhold information, avoid certain providers, or even reject digital innovation (Kurniawan et al., 2024).

The lack of institutional accountability perpetuates inequities between large and small facilities. Larger institutions with greater resources can endure the reputational impact of violations without significant financial penalties, while smaller clinics, which may be more vulnerable to scrutiny, often have less bargaining power and weaker defense mechanisms. This imbalance creates a regulatory gap where law enforcement disproportionately affects weaker actors, while larger actors can continue to operate without significant changes to their systems or governance structures.

Therefore, strengthening institutional sanctions is crucial to aligning practice with policy. Sanctions that include financial fines, public disclosure of violations, license suspension, or mandatory corrective action plans will create stronger incentives for compliance. More importantly, shifting accountability from individuals to institutions ensures that healthcare organizations cannot evade responsibility by scapegoating staff. Only when institutions face direct consequences will they begin to prioritize comprehensive reforms, investing in secure digital infrastructure, embedding privacy protections into workflows, and fostering a culture of accountability at every level of care (Dalimunthe & Simarmata, 2021).

The Urgency of Policy and Oversight Reform

Indonesia urgently and critically needs to achieve stronger harmonization and integration of its various legal instruments governing health data protection. Currently, the country's regulatory landscape consists of several overlapping laws and regulations, such as the Personal Data Protection (PDP) Law No. 27 of 2022, the recently enacted Health Law No. 17 of 2023, the Electronic Information and Transactions (ITE) Law, and Minister of Health Regulation No. 24 of 2022 on Medical Records. While each of these frameworks aims to protect personal and health data, their fragmented nature often results in ambiguity, inconsistent application, and gaps in enforcement. This complexity complicates the ability of healthcare facilities and regulators to consistently interpret, comply with, and enforce important data protection standards. The lack of regulatory cohesion can also create gaps, where some health data practices fall outside of clear legal oversight or accountability (Azwar & Sirait, 2025).

By establishing updated standards to strengthen data security in the healthcare sector, including digital healthcare services such as telemedicine, Indonesia's 2023 Health Law represents a major step forward. This law complements and aligns with the Personal Data Protection (PDP) Law, which specifically categorizes health data as sensitive personal data requiring enhanced security and privacy protection. Together, these laws impose clear obligations on healthcare providers as data controllers to safeguard patient confidentiality, security, and rights. However, the full potential of these improvements can only be realized if legal instruments are fully integrated to avoid regulatory conflicts or uncertainty. For example, the Health Law's mandates for health information system providers and data security must function seamlessly with the broader data management principles in the Personal Data Protection Law, as well as the protection of electronic information in the ITE Law.

Indonesia can learn important lessons from international models, such as the European Union's General Data Protection Regulation (GDPR), which combines various data protection rules into a single,

comprehensive legal framework with clear definitions, enforcement mechanisms, and accountability structures. GDPR integration helps address the fragmentation seen in previous European data protection regimes, facilitating better compliance and more effective regulation of personal data, including health data, across all sectors (Absori Absori, Hernanda, Wardiono, Fitriciada, & Budiono, 2023). Similarly, Indonesia's health data protection framework needs to be better integrated to provide a clear, cohesive, and enforceable legal basis for healthcare institutions. This would enable easier regulation of electronic medical records, telehealth services, and other new digital health innovations in a rapidly evolving technological environment (Rahayu, 2025).

Furthermore, the integration of these laws must be supported by standardized operational protocols and guidelines to encourage consistent implementation across Indonesia's vast and diverse healthcare system. Integrated policies will also streamline the responsibilities of regulatory bodies, such as the Ministry of Health, the Ministry of Communication and Informatics, and the Personal Data Protection Authority, to coordinate monitoring, auditing, and enforcement. By eliminating regulatory overlap and contradictions, stronger harmonization can reduce confusion for healthcare providers and empower regulators to act decisively against privacy violations. Ultimately, comprehensive legal integration will strengthen patient trust and confidence in Indonesia's healthcare data management system, while protecting privacy and individual rights in the digital age (K. Wardiono et al., 2021).

In short, while Indonesia's health data protection legal framework has developed rapidly, the pressing challenge lies in achieving a cohesive and integrated regulatory environment. Learning from international best practices and integrating the principles and procedures outlined in the PDP Law, the Health Law, the ITE Law, and ministerial regulations will be essential to ensure that the Indonesian health sector benefits from robust data protection that keeps pace with rapid technological changes and respects patient rights (Kurniawan et al., 2024).

Security Certification of Medical Information Systems

With the increasing digitization of healthcare data, the need for robust security measures to protect sensitive patient information becomes increasingly critical. Healthcare information systems, including Hospital Management Information Systems and telemedicine platforms in Indonesia, must comply with stringent security certification requirements. This certification serves as a critical benchmark to verify that the systems implement robust technical safeguards against cyber threats, including unauthorized access, data breaches, and data manipulation.

Security certification for medical information systems typically requires verification of several critical security components. These include robust data encryption protocols to protect data confidentiality during storage and transmission, the installation of advanced firewalls to protect the system from unauthorized external access, and comprehensive vulnerability assessments to identify and mitigate potential security vulnerabilities. These assessments help ensure that healthcare systems maintain robust defenses against evolving cyberattack techniques and comply with legal and ethical mandates to safeguard patient privacy.

To provide a reliable and standardized approach to securing healthcare information, certification can be aligned with internationally recognized frameworks, such as the ISO/IEC 27001 standard. This certification outlines a global benchmark for information security management systems, which encompasses policies, procedures, technical controls, and organizational structures designed to systematically protect sensitive data. By aligning Hospital Management Information Systems and telemedicine platforms with ISO standards, Indonesia can ensure that these healthcare IT systems meet national regulations and global best practices, thereby fostering greater trust among patients, providers, and regulators.

The certification process also encourages healthcare institutions to instill a security-focused culture and a mindset of continuous improvement at all levels of their operations (Arief Budiono, Absori, Wardiono, Yuspin, & Gulyamov, 2023). Achieving and maintaining certification involves regular audits, security policy reviews, incident response planning, and staff training on data security awareness. These practices not only directly improve system security but also enhance the healthcare sector's overall readiness to respond to emerging threats, minimizing the impact of potential breaches on patient care (A Absori, Hernanda, Fitriciada, Wardiono, & Budiono, 2023).

Additionally, mandatory security certification could be a prerequisite for healthcare providers offering electronic medical records and telemedicine services (Hartotok, Absori, Dimyati, Santoso, & Budiono, 2021). Requiring certified systems ensures that only platforms capable of protecting sensitive

medical information are implemented, thereby reducing systemic vulnerabilities. It also incentivizes technology vendors and healthcare institutions to prioritize security in their IT infrastructure investments and strategies (Izziyana et al., 2019).

The implementation of mandatory security certification for healthcare information systems will strengthen Indonesia's commitment to data protection amidst rapid digital transformation. This will support compliance with applicable legal requirements under the PDP Law and Minister of Health Regulation 24/2022, increase patient trust in digital healthcare services, and align national healthcare data security practices with international standards, thereby contributing to the resilience and integrity of the Indonesian healthcare ecosystem (Novianti & Bakhtiar, 2024).

Periodic Audits and Multi-Sectoral Supervision

Regular audits conducted by regulatory bodies are a crucial component of a robust health data protection system. In Indonesia, oversight mechanisms need to be revitalized to ensure effective enforcement of laws and policies related to the protection of medical records. Regular audits should ideally be conducted by key institutions, such as the Ministry of Health and the Ministry of Communication and Informatics (Hernanda et al., 2023). Their efforts should be coordinated and synchronized with other relevant institutions, such as the Social Security Agency and the Financial Services Authority, to cover the full spectrum of healthcare delivery, insurance claims, and financial transactions involving medical data (Arief Budiono, Absori, Ngestiningrum, & Nugroho, 2018).

This audit should be comprehensive, evaluating both the technical and operational aspects of the health information system. From a technical perspective, the audit should assess security measures, such as data encryption, firewall protection, and data management (A. Budiono et al., 2019). Simultaneously, operational audits should review whether healthcare facilities are following established procedures for data entry, consent management, data sharing, breach notification, and staff training on privacy compliance. Such dual-focus audits identify not only technological weaknesses but also human and procedural factors that could lead to data breaches or misuse (Yuspin, Wardiono, Nurrahman, & Budiono, 2020).

Importantly, both scheduled audits and unannounced inspections can serve as effective deterrents against complacency and negligence. Routine audits enable institutions to prepare and ensure consistent compliance, while periodic unannounced audits provide regulators with a clear picture of actual day-to-day practices. International experience shows that this dual approach strengthens institutional accountability and incentivizes healthcare providers to remain vigilant in managing patient data security. This approach also provides regulators with clear evidence to enforce sanctions, implement corrective actions, or recommend systemic improvements when violations are detected.

Furthermore, routine audit results must be reported transparently to maintain public trust and drive sector-wide improvements. Collaboration between the Ministry of Health, ICT authorities, the Social Security Agency, and financial regulators could also facilitate the creation of a unified dashboard or reporting system that tracks compliance trends and incidents at a national scale. This unified oversight structure would help close enforcement gaps, encourage the harmonized implementation of data protection laws, and support the development of targeted capacity-building programs for healthcare providers.

Regular and comprehensive audits conducted by an authorized and coordinated regulatory body are essential to improving data protection in Indonesia's healthcare sector. These audits enable timely identification of vulnerabilities, enforce legal compliance, and foster a culture of accountability. All of this is crucial to ensuring patient records are managed responsibly in an increasingly digital healthcare environment (Sadnyini et al., 2024).

Conclusion

The study found that while existing frameworks for protecting patient data are currently in place, their implementation is far from ideal. The Personal Data Protection Law, Health Law No. 17 of 2023, and other legislation must be combined with stricter enforcement procedures, more frequent audits, and strict sanctions. Other ways to build digital capabilities include implementing secure and integrated electronic medical records, educating healthcare professionals about medical data ethics and legal regulations, and building a culture of transparency to enhance accountability. By taking these steps, patient data security can be enhanced, the risk of misuse can be reduced, and public trust in healthcare services can be maintained.

Acknowledgements

The authors would like to thank Universitas Muhammadiyah Surakarta and Mamun University.

References

[1] Absori, A, Hernanda, T., Fitriciada, A., Wardiono, K., & Budiono, A. (2023). Analysis of the Issues on Bengawan Solo River Basin Management Policies. WSEAS Transactions on Environment and Development, 19, 25–32. https://doi.org/10.37394/232015.2023.19.3

[2] Absori, Absori, Hernanda, T., Wardiono, K., Fitriciada, A., & Budiono, A. (2023). Critical analysis of River Basin Management Regulation in Bengawan Solo for Water Tourism: Local Legislation in 7 Regency. WSEAS Transactions on Environment and Development, 19, 844–851. https://doi.org/10.37394/232015.2023.19.80

[3] Anwar, T. M., Tambun, J. G., & Jaeni, A. (2025). Juridical Analysis of the Misuse of Electronic Medical Records in the Perspective of the Electronic Information and Transaction Law. Pranata Hukum, 20(1). https://doi.org/10.36448/pranatahukum.v20i1.380

[4] Azwar, T. K. D., & Sirait, N. N. (2025). The Legal Framework for Personal Data Protection Amidst Hospital Competition: Ensuring Patient Safety in the Era of Healthcare Digitalization. Proceedings of the 1st International Conference on Social Environmental Diversity, 416–426. https://doi.org/10.2991/978-2-38476-366-5_38

[5] Benuf, K., & Azhar, M. (2020). Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer (Legal Research Methodology as an Instrument for Resolving Contemporary Legal Issues). Jurnal Gema Keadilan, 7(1), 145–160. https://doi.org/10.14710/gk.2020.7504

[6] Budiono, A., Absori, Harun, H., Nugroho, H. S. W., Dimyati, K., Ngestiningrum, A. H., & Izziyana, W. V. (2019). The anachronism of the Indonesian social security policy in health. Medico-Legal Update, 19(1). https://doi.org/10.5958/0974-1283.2019.00046.X

[7] Budiono, Arief, Absori, A., Ngestiningrum, A. H., & Nugroho, H. S. W. (2018). Pseudo National Security System of Health in Indonesia. Indian Journal of Public Health Research & Development, 9(10), 556–560. https://doi.org/10.5958/0976-5506.2018.01404.3

[8] Budiono, Arief, Absori, Wardiono, K., Yuspin, W., & Gulyamov, S. S. (2023). Cyber Indoctrination Victims in Indonesia and Uzbekistan: Victim Protection and Indoctrination in Practice. Journal of Human Rights, Culture and Legal System, 3(3), 441–475. https://doi.org/10.53955/jhcls.v3i3.127

[9] Dalimunthe, W., & Simarmata, M. (2021). Patient Legal Protection in the Digital Era and a Study of Telemedicine Services in Indonesia. Journal of Legal Sciences, 10(1), 40–49. https://doi.org/10.30596/dll.v10i1.22494

[10] Hartotok, H., Absori, A., Dimyati, K., Santoso, H., & Budiono, A. (2021). Stunting prevention policy as a form of child health rights legal protection. Open Access Macedonian Journal Medical Sciences, 9, 1218–1223. https://doi.org/10.3889/oamjms.2021.7254

[11] Hernanda, T., Absori, Wardiono, K., Azhari, A. F., Arlinwibowo, Janu Azizah, N., & Budiono, A. (2023). The Impact of Environmental Regulation Implementation: A Meta-Analysis. International Journal of Sustainable Development and Planning, 18(10), 3235–3242. https://doi.org/10.18280/ijsdp.181023

[12] Izziyana, W. V., Harun, Absori, Wardiono, K., Nugroho, H. S. W., & Budiono, A. (2019). Health insurance for Indonesian migrant workers. Medico-Legal Update, 19(1), 188–192. https://doi.org/10.5958/0974-1283.2019.00038.0

[13] Jiwanti, A., & Soponyono, E. (2022). The Urgency of Judge's Legal Reasoning in Deciding on an Environmental Crime Case Based on an Ecocentric Approach (Review of Case Decision No. 640/PID.B/LH/2021/PT PBR). Jurnal Jurisprudence, 12(2), 71–91.

[14] Komalasari, R., & Mustafa, C. (2024). Electronic Health Records in Indonesia: A Law and Policy Analysis. Ibn Chaldun University Journal, 2.

[15] Kurniawan, K. D., Hehanussa, D. J., Setiawan, R., Susilowati, I., & Helfisar, D. (2024). Criminal Sanctions and Personal Data Protection in Indonesia. Lex Publica, 11(2), 221–247.

[16] Larasati, T., Fardiansyah, A. I., Saketi, D., & Dewiarti, A. N. (2024). The ethical and legal aspects of health policy on electronic medical records in Indonesia. Cepalo, 8(2), 103–112. https://doi.org/10.25041/cepalo.v8no2.3634

[17] Lukitasari, D. A., Huda, M. K., & Asmuni. (2023). Hospital Legal Responsibilities Against Misuse of Patient Personal Data in Electronic Medical Records. JILPR Journal of Indonesia Law & Policy Review, 5(1).

[18] Marwiyah. (2022). Analysis Of Legal Review Of Medical Information Release To Ensure The Confidentiality Of Patient Identity. Awang Long Law Review, 4(2), 326–330.

[19] Novianti, & Bakhtiar, H. S. (2024). Implementation of Electronic Medical Record System in Indonesia Viewed from the Perspective of Legal Certainty. International Journal of Engineering Business and Social Science, 2(4), 2980–4272. Retrieved from https://ijebss.ph/index.php/ijebss

[20] Rahayu, W. (2025). Legal Framework For Health Data Protection: Balancing Patient Privacy and Institutional Needs. International Journal of Health Administration Law and Government Policies, 1(1). Retrieved from https://journal.univummibogor.ac.id/index.php/IJHALGP

[21] Ramadianto, A. Y. (2023). Patient's Right to Obtain The Electronic Medical Record Contents in Therapeutic Contract According to Indonesian Civil Law Perspective Anggra Yudha Ramadianto. West Science Law and Human Rights, 1(3), 122–132.

[22] Ratnawati, A., & Iskandar, D. (2025). Constraints in the Implementation of Electronic Medical Records at Community Health Centers in Accordance with Permenkes 24 of 2022. Saintika Medika, 21(1), 27–45. https://doi.org/10.22219/SM.VOL21.SMUMM1.40368

[23] Roro, R., Satyoputri, J., & Sidi, R. (2024). Electronic Medical Records: Legal Protection and Challenges in Health Services in Hospitals. Berpusi Publishing.

[24] Sadnyini, I. A., Christianto, D., Kurniawan, I. G. A., & Jayantara, M. (2024). Legal Approaches for Clinical Audits and Sanctions in Indonesian Health Service Facilities. Jurnal Hukum Prasada, 11(1), 16–24. https://doi.org/10.22225/jhp.11.1.2024.16-24

[25] Soekanto, S. (2012). Pengantar Penelitian Hukum (Introduction to Legal Research). Jakarta: Universitas Indonesia Press. Retrieved from https://simpus.mkri.id/opac/detail-opac?id=8443

[26] 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

[27] Wardiono, K., Dimyati, K., Nugroho, S. S., Nugroho, H. S. W., Acob, J. R., & Budiono, A. (2021). Philosophy, Law, and Ethics of Handling Covid-19 Pandemic in Indonesia. Open Access Macedonian Journal of Medical Sciences, 9, 1104–1108.

[28] Wardiono, Kelik. (2019). Prophetic: An Epistemological Offer for Legal Studies. Journal of Transcendental Law, 1(1), 17–41. https://doi.org/10.23917/jtl.v1i1.8797

[29] Widjaja, G. (2025). A Critical Study Of Landmark Cases In The Legal Protection Of Medical Personnel And Patients In Indonesia. Berajah Journal, 5(1), 13–20. https://doi.org/10.47353/BJ.V5I1.553

[30] Wiraguna, S. A. (2025). Exploration Of Research Methods With Normative And Empirical Approaches In Legal Research In Indonesia. Lex Jurnalica, 22(1), 66.

[31] Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2020). The ideal management of health insurance for Indonesia according to constitution. Quality - Access to Success, 21(176), 48 – 50.