**JURISPRUDENSI**
Jurnal Ilmu Syari'ah, Perundang-undangan dan Ekonomi Islam
https://doi.org/10.32505/jurisprudensi.v16i2.13234
Vol. 17 No. 2 (Juli-Desember 2025): 350-366

# Principle of Consent in the Protection of Medical Personnel's Personal Data: Implications and Consequences

**Juan Ponce Enrile Febriansyah** [1]
Universitas Tarumanagara, Jakarta, Indonesia
enrilefebriansyah2@gmail.com

**Ida Kurnia**
Universitas Tarumanagara, Jakarta, Indonesia
idah@fh.untar.ac.id

| Submission | Accepted | Published |
|---|---|---|
| Des 3, 2025 | Des 7, 2025 | Des 8, 2025 |

***Abstract***

*Ideally, the principle of consent serves as the ethical and legal foundation for managing the personal data of medical personnel to ensure that every sensitive piece of information is processed transparently and securely. However, practical realities reveal weak compliance, limited awareness of data rights, and the rapid development of health technologies that are not yet balanced with adequate regulation. These conditions give rise to various legal issues, including data breaches and misuse of information that may harm medical personnel both personally and professionally. This study aims to analyze the position of the consent principle as one of the key pillars of personal data protection for medical personnel, while also outlining the implications and legal consequences of its implementation within the context of modern healthcare services. The methodology used in this study is categorized as qualitative library research, employing a normative legal approach explained through descriptive-analytical analysis. The findings indicate that the fulfillment of the consent principle has not been fully effective and still requires regulatory strengthening, enhanced data literacy, and consistent law enforcement to safeguard the integrity and security of medical personnel data.*

***Keywords:*** *Principle of Consent, Data Protection, Medical Personnel*

[1] Corresponding Author

**Abstrak**

Idealnya, prinsip persetujuan menjadi dasar etis dan hukum dalam pengelolaan data pribadi tenaga medis agar setiap informasi sensitif diproses secara transparan dan aman. Namun, praktik di lapangan menunjukkan lemahnya kepatuhan, rendahnya pemahaman hak atas data, serta pesatnya teknologi kesehatan yang belum diimbangi regulasi memadai. Kondisi ini memunculkan berbagai persoalan hukum, termasuk kebocoran dan penyalahgunaan data yang merugikan tenaga medis secara personal maupun profesional. Penelitian ini bertujuan untuk menganalisis kedudukan prinsip persetujuan sebagai salah satu pilar utama perlindungan data pribadi tenaga medis, sekaligus menguraikan implikasi serta konsekuensi yuridis dari penerapannya dalam konteks pelayanan kesehatan modern. Metodologi yang digunakan dalam penelitian ini tergolong dalam penelitian pustaka berbasis kualitatif, di mana metode yang digunakan adalah studi hukum normatif yang dijelaskan secara deskriptif analitis. Temuan penelitian menunjukkan bahwa pemenuhan prinsip persetujuan belum sepenuhnya efektif dan masih membutuhkan penguatan regulatif, peningkatan literasi data, serta penegakan hukum yang konsisten demi melindungi integritas dan keamanan data tenaga medis.

**Kata kunci:** Perinsip Persetujuan, Perlindungan Data, Tenaga Medis

## Introduction

The digitalization of the health sector over the past decade has created a new landscape in information management, where data has become a primary asset for improving service quality, research, and health governance. This transformation has produced increasingly integrated systems, ranging from electronic medical records, national health platforms, telemedicine services, to medical workforce management applications that connect various institutions in real time (Punia, 2025). Within this technological architecture, personal data is no longer merely an administrative record but has evolved into a digital representation that determines access, professional status, and an individual's track record within the health system. Medical personnel—doctors, nurses, midwives, and allied health professionals—are deeply embedded in this ecosystem, as their identities and professional information are stored, linked, and processed for multiple purposes. Amid these developments, fundamental questions arise regarding how the personal data of medical personnel is protected, how it is processed, and the extent of control granted to the individuals who own the information. These questions are crucial given that digital health systems offer significant benefits while also presenting considerable risks if not managed carefully.

The issue of protecting the personal data of medical personnel cannot be separated from the principle of consent as a key pillar in data protection regulation. This principle requires clear, specific, and informed permission from medical personnel before their data is collected, used, or disseminated

(Herisasono, 2024). However, in the highly complex health sector, the principle of consent cannot be interpreted simplistically. The data of medical personnel is used not only for administrative purposes such as identity verification or scheduling but also for performance analysis, medical audits, health research, and quality control of services. The use of data that extends beyond its initial purpose of collection makes the principle of consent a norm that must be carefully construed (Rosadi, 2017). Operating in a field directly tied to public safety, medical personnel carry dual identities: as data subjects entitled to protection, and as public professionals whose actions cannot be entirely shielded from public scrutiny. This ambiguity demands more elaborative regulation and rigorous implementation.

Ideally, the principle of consent should serve as a mechanism that balances the public's need for transparency in healthcare with the rights of medical personnel to control their personal data. However, reality reveals a situation far from ideal. Numerous cases of data breaches, exposure of medical personnel's identities in criminal reporting, misuse of digital records, and unrestricted publication of professional histories illustrate that consent often becomes a mere administrative formality (Supriyadi, 2023). In many institutions, medical personnel lack genuine choice and are compelled to consent to extensive data processing without clarity on purposes, limitations, or control mechanisms. In other circumstances, consent is deemed irrelevant when information about medical personnel is considered related to public interest, allowing data to be widely disclosed without regard for proportionality or data minimization. This gap between the ideal concept and actual practice constitutes the core problem addressed in this research, namely how the principle of consent is applied, neglected, or misunderstood in the protection of medical personnel's personal data.

The purpose of this research is to analyze the position, role, and mechanisms of the principle of consent in protecting the personal data of medical personnel, as well as to evaluate the implications and consequences arising from its implementation or neglect. This study aims to identify the legal framework regulating consent in the context of data protection, assess data management practices involving medical personnel within the digital health system, and reveal the risks and challenges that emerge when consent is not properly executed. Additionally, this research seeks to propose a more pragmatic perspective on how the principle of consent can be effectively implemented without hindering digital health innovation or undermining the rights of medical personnel as data subjects.

The contribution of this research lies in its effort to provide a more comprehensive understanding of the urgency of the principle of consent for medical personnel within an increasingly complex digital health ecosystem. By integrating legal, ethical, and practical analyses, this study offers conceptual and argumentative foundations that can guide policymakers, health institutions, professional organizations, and digital health platforms in formulating data protection standards that are more equitable and proportional. This research also contributes to strengthening the body of literature on data protection in Indonesia, particularly in the context of medical personnel—which has so far received limited explicit attention—so that the findings may serve as a basis for developing policies that respect privacy while safeguarding public interests in healthcare services.

## Literature Review

Studies on the protection of the personal data of medical personnel are not entirely new, as several authors have examined and discussed this issue from various perspectives and methodological approaches. Lineus Frederico et al., in their work titled; *"Perlindungan Hukum Terhadap Data Pasien Sebagai Jaminan Atas Data Pribadi Dalam Pelayanan Kesehatan",* discuss how patient data must be managed based on principles of security, confidentiality, and consent as part of patients' fundamental rights in healthcare services. Their study emphasizes that the protection of patient data constitutes a legal obligation that hospitals and health practitioners must fulfill under the Health Law and medical record regulations. The key finding of the study reveals that weak data management systems and the absence of adequate access control mechanisms are the primary causes of patient data breaches (Frederico et al., 2024). The similarity between that study and the present research lies in the shared emphasis on the importance of consent as the legal basis for personal data processing. However, the difference is that their study focuses on patients as data subjects, whereas the present research highlights medical personnel, whose roles involve distinct ethical and professional dimensions as well as more complex risks of public exposure.

Handryas Prasetyo Utomo et al., in their work titled; *"Urgensi Perlindungan Hukum Data Pribadi Pasien dalam Pelayanan Kesehatan Berbasis Teknologi di Indonesia",* examine how the advancement of information technology in healthcare services creates significant challenges to the confidentiality of patients' personal data. Their research maps the risks of data processing within digital health systems, including electronic medical records and online health applications. The main finding shows that the national regulations at the time were insufficient to provide comprehensive protection for patients' personal data, indicating the need for improved legal instruments and stronger digital health governance (Utomo et al., 2020). The similarity with the present study lies in the shared concern over data-processing risks within technology-driven health ecosystems. The difference is that their research centers on patient protection in the context of technological development, while the present study expands the analysis to medical personnel, including issues of reputation, public exposure, and the integration of professional data—areas not previously explored.

Julsandri, in the work titled; *"Legal Aspects of Protecting Patient Medical Data in the E-Puskesmas System",* analyzes legal protection for patient medical data within the e-Puskesmas system, focusing on system vulnerabilities, legal compliance, and the implementation of data protection policies at the regional level. The findings reveal that the e-Puskesmas system still has numerous technical and procedural weaknesses, which increase the risk of data breaches and hinder the optimal implementation of privacy principles in practice (Julsandri, 2025). Its similarity with the present study lies in raising concerns about the effectiveness of data protection in digital health systems. The difference, however, is the scope of analysis: Julsandri's research is limited to patient data within the e-Puskesmas system, whereas the present research extends the discussion to medical personnel, whose data include professional identities, disciplinary records, and potential public exposure in legal cases or media reporting.

Based on the existing body of research, a clear research gap emerges, namely the lack of studies specifically addressing the principle of consent within the context of protecting the personal data of medical personnel. All previous studies focus on patients as data subjects, whereas medical personnel face distinct dynamics: risks of professional data exposure, links to disciplinary or criminal processes, cross-platform data integration, and far more complex reputational consequences. Furthermore, no prior study has thoroughly analyzed the technological and social implications of neglecting the principle of consent for medical personnel within the national digital health system. Therefore, the present research fills this gap by providing a more targeted, comprehensive, and contextual analysis of how the principle of consent should be understood and implemented in protecting the personal data of medical personnel, along with its implications and consequences.

## Research Methodology

This article falls within qualitative library research, employing a normative legal study method explained through descriptive–analytical analysis (Benuf & Azhar, 2020). The normative legal research is conducted by systematically examining primary legal materials such as the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 on Personal Data Protection, the Health Law, the Medical Practice Law, Minister of Health Regulation Number 24 of 2022 on Medical Records, as well as various technical regulations governing data governance and the professional practices of medical personnel. Secondary sources include books on privacy law, scholarly journals on health data protection, academic publications on health digitalization, and research reports related to data breaches and the governance of digital health systems. Tertiary sources are used to strengthen conceptual interpretation, consisting of legal dictionaries, encyclopedias, and indexes that help clarify conceptual definitions in the discussion. All legal materials were not only collected but also organized through in-depth reading to identify inter-norm relationships and to assess the position of the consent principle within the broader framework of protecting the personal data of medical personnel.

Data analysis was carried out using a descriptive qualitative approach with a deductive reasoning technique, beginning with general legal principles and testing them against concrete cases such as medical personnel data breaches, public exposure of professional information, and data processing within national digital health platforms. Data validity was ensured through source triangulation by comparing legal norms in regulations, court decisions, and academic literature to confirm consistency between legal rules and actual practices. Validation was further strengthened by examining the coherence of norms through cross-checking interconnected sectoral regulations such as the PDP Law, the Health Law, and Minister of Health Regulation 24/2022 to identify potential overlaps or normative gaps. The process of synthesizing data into a structured narrative was carried out through legal interpretation techniques emphasizing argumentative clarity, systematic norm mapping, and direct linkage between theoretical issues and empirical problems, ensuring that the discussion produced is not merely textual

but also analytical and contextual in describing the position of the consent principle in the protection of medical personnel's personal data.

## Protection of Medical Personnel's Personal Data

The protection of medical personnel's personal data is one of the essential dimensions of modern health governance, which is becoming increasingly digitalized. Conceptually, personal data protection refers to a set of principles, mechanisms, and policies designed to ensure that identifiable information is processed lawfully, securely, proportionally, and in accordance with legally justified purposes (Fahmanadie et al., 2025). This definition becomes more complex when applied within the health sector, because the personal data of medical personnel not only includes general identifiers such as name, address, or identification numbers, but also professional data that has direct implications for their integrity, reputation, and credibility as healthcare providers. Thus, the protection of medical personnel's personal data cannot be understood merely as an administrative issue, but also as an ethical, juridical, and social matter that affects their position within the health system.

The core issues that arise in the protection of medical personnel's data stem from two important realities. First, the health sector is the ecosystem most saturated with sensitive information—both patient and medical personnel data—making the risk of misuse or data breaches far higher compared to other sectors. Second, massive digital transformation—through electronic medical records, national platforms such as *SatuSehat*, and telemedicine—has expanded the scope of data processing and created a new need for more stringent data governance (Punia, 2025). At this point, the issue is no longer merely whether the data is collected properly, but how it is used, who has the authority to access it, for what purposes the processing is conducted, and how oversight is implemented. Without a strong protection framework, medical personnel face risks that are not only legal in nature, but also reputational and psychological.

The context of medical personnel as data subjects carries its own distinct characteristics. They are not only owners of personal data but also individuals who process patients' health data every day, placing them in a dual position: as protectors of others' data and as individuals whose own data must be protected. Professional data such as registration and practice license numbers (STR and SIP), training records, disciplinary history, and performance evaluations form part of their digital profile, which is linked to various institutional systems including hospitals, professional organizations, the Ministry of Health, and digital health applications (Swede et al., 2019). This interconnectedness increases the potential exposure of personal data through system leaks, uncontrolled internal access, or dissemination of data in the context of public reporting. In certain circumstances—such as alleged ethical violations, disciplinary findings, or criminal cases—data belonging to medical personnel may easily shift from administrative spaces to the public sphere without clear boundaries.

On the other hand, medical personnel have a fundamental need to maintain their professional dignity. Reputation and credibility are not merely personal attributes but ethical requirements that shape public trust in healthcare services.

When their personal or professional data is disseminated without legal basis or without clear purpose limitations, the impact can be far more severe than for employees in other sectors. Information taken out of context—such as preliminary reports, unverified allegations, or disciplinary data still under review—can cause reputational damage that is difficult to repair (Winkler et al., 2025). This situation shows that the protection of medical personnel's data is directly related to procedural justice and the presumption of innocence, which are foundational principles of a fair legal system.

Given this complexity, the protection of medical personnel's personal data must be understood as a foundation for a healthy relationship between the state, healthcare institutions, and the medical personnel themselves. Every digital health policy—from the integration of electronic medical records to the development of healthcare workforce data systems—must consider the risks and potential impacts arising from uncontrolled data processing. Here, fundamental principles of data protection such as purpose limitation, data minimization, processing security, accountability, and transparency play a crucial role in ensuring that data collection and use do not infringe upon the basic rights of medical personnel. Concepts such as *privacy by design* and *privacy by default* must be embedded within the architecture of digital health systems so that data protection is not merely a formal regulation but a technical practice applied in daily operations.

## Regulation and Implementation of the Consent Principle in the Protection of Medical Personnel's Personal Data

The regulation and implementation of the consent principle in protecting the personal data of medical personnel has become increasingly important as digitalization in healthcare services expands and data integration within national systems continues to grow. In general, personal data protection is part of broader efforts to uphold individual dignity and autonomy—including that of doctors and nurses—in facing the risks of data misuse in the digital transformation era. This principle gains strong normative grounding through Law Number 27 of 2022 on Personal Data Protection (the PDP Law), which affirms that data processing may only be carried out on the basis of lawful grounds (Saly et al., 2023). Thus, consent is not merely an administrative formality; it is a crucial instrument that ensures medical personnel retain control over their personal data amid increasingly complex and large-scale integration of healthcare systems.

More specifically, the PDP Law defines personal data as information regarding an identified or identifiable individual, including health data as a category of "specific personal data" that requires heightened protection. For medical personnel, personal data includes not only general identifiers but also professional information such as registration and practice license numbers (STR and SIP), educational history, competency records, disciplinary files, and even personal health information. With their dual position as data subjects and as processors of patient data, doctors and nurses require a more sensitive consent framework—one that not only protects patients but also recognizes their autonomous rights over their professional and personal data. Without such a

mechanism, medical personnel risk becoming subjects of surveillance and control rather than individuals whose rights are safeguarded.

The PDP Law also stipulates that the processing of specific personal data such as health data generally requires explicit consent from the data subject, except in certain conditions permitted by law, such as in the public interest for healthcare, state legal obligations, or law enforcement purposes. In the context of medical personnel, this means that the management of their data by hospitals, the Ministry of Health, insurance companies, professional organizations, and digital health platforms should be carried out transparently (Rizqiyanto et al., 2024). The purposes of processing, types of data involved, retention duration, legal basis, and potential data sharing with third parties must be clearly communicated. Any processing unrelated to core professional duties ideally returns to specific, informed, and freely given consent, as mandated by the PDP Law.

However, when these principles are applied within sectoral health regulations, a shift in focus becomes evident: protections are oriented more toward patient data rather than medical personnel as data subjects. Although the Health Law and the Medical Practice Law emphasize the obligation to maintain confidentiality, their orientation leans heavily toward protecting patient information. The position of medical personnel as individuals who also have privacy and data protection rights is not proportionately addressed. Regulations detailing how their professional data, competency records, or personal information may be processed or disclosed are largely absent. This regulatory gap complicates the implementation of the consent principle, as it remains unclear when and how medical personnel may grant or refuse consent regarding the use of their own data.

One relevant technical regulation is Ministry of Health Regulation Number 24 of 2022 on Medical Records, which governs the integration of electronic medical records through national platforms such as SatuSehat. This regulation obligates healthcare facilities to upload medical records into a centralized system that includes the identities of medical personnel providing care (Rizqiyanto et al., 2024). In this context, data such as names, registration numbers, specialization, and other professional attributes are automatically integrated into national systems. The legal basis for such data processing is no longer individual consent from medical personnel but structural legal obligations. As a result, consent is not the primary basis for processing, giving the impression that national system needs override the individual's control over their own data.

Although the PDP Law allows "public interest" or "state obligations" as substitutes for consent, such bases do not eliminate the data controller's obligation to comply with all data protection principles, including purpose limitation, transparency, and accountability. Consequently, the Ministry of Health and healthcare facilities remain responsible for determining the scope of medical personnel data to be processed, specifying who may access it, setting boundaries for public disclosure of professional information, and providing mechanisms for objections and data deletion. Without these components, medical personnel lose the ability to exercise meaningful control, despite being data subjects who have the right to determine the boundaries of their personal information.

Nevertheless, Regulation No. 24/2022 focuses more heavily on the technical aspects of integration and electronic medical record implementation rather than strengthening the rights of medical personnel as data owners. It contains no explicit provisions granting medical personnel the right to approve or refuse the use of their data beyond the context of care delivery (Siregar, 2024). Mechanisms for restricting access or limiting the publication of professional profiles are also absent. As a result, the consent principle—intended to be central to personal data protection—becomes overshadowed by system integration priorities and administrative interests. This renders the consent requirement mandated by the PDP Law less visible in practical implementation.

In modern data protection discourse, the concepts of *privacy by design* and *privacy by default* offer a more progressive approach that could strengthen the position of medical personnel. These principles require that data protection and consent mechanisms be embedded at the system design stage, not merely added as administrative requirements. If applied within systems such as SatuSehat, there would be features enabling medical personnel to control the extent to which their data may be processed or displayed. The system should also provide opt-in and opt-out options for secondary processing purposes such as research, policy analysis, or professional profile publication. Unfortunately, such approaches are not yet evident within Indonesia's digital health architecture.

Current realities show that the design of digital health systems still prioritizes administrative efficiency and data integration rather than the protection of medical personnel's autonomy. No consent module exists that allows medical personnel to control the use of their data (Damayanti et al., 2025). There are no clear provisions on whether medical personnel may restrict access to disciplinary information or whether they must be notified when their data is used for audits or research. This reveals a significant gap between the normative principles established in the PDP Law and the technocratic, bureaucratic implementation prevalent in the health sector.

Research findings on telemedicine further reinforce the picture that digital health regulation lags behind technological practice. Studies indicate that telemedicine regulations in Indonesia remain weak in terms of legal substance, institutional framework, and legal culture, rendering such services high-risk. Many norms remain temporary and have not been elevated into permanent legislation. This reflects a recurring pattern: technological innovation progresses rapidly while legal frameworks protecting medical personnel develop slowly (Guamo, 2025). As a result, the consent principle becomes subordinate, overshadowed by the efficiency demands of digital services that integrate data massively without providing adequate control to medical personnel as data subjects.

In daily practice, hospitals and digital platforms often rely on broad, general consent clauses in employment contracts or terms of use as a justification for processing medical personnel data. Such consent is sweeping and does not distinguish between different processing purposes. Medical personnel are deemed to have agreed to all forms of processing merely because they work in an institution or use a particular platform. This practice contradicts the PDP Law's requirement that consent must be specific, informed, and purpose-bound. This ambiguity blurs the line between institutional authority and the autonomous

rights of medical personnel, weakening their position as legal subjects who hold rights over their own personal data.

**Implications of Implementing or Ignoring the Consent Principle in the Protection of Medical Personnel Data**

The principle of consent in personal data processing is a foundational element that determines the legitimacy of any form of collection, use, and dissemination of information—especially within the healthcare sector, which is saturated with sensitive data. In the context of medical personnel, consent plays an even more critical role because their data concerns not only identity but also professional integrity, ethical track records, and medical practice histories. When this principle is weakly applied or entirely disregarded, the issue extends beyond administrative error and may escalate into legal violations that undermine the professional dignity of doctors and nurses (Sylviana et al., 2025). Thus, the implementation or neglect of the consent principle carries far-reaching implications that must be understood comprehensively from both legal and practical perspectives within an increasingly digitalized health system.

In the legal dimension, the neglect or inadequate application of the consent principle may trigger administrative, civil, or even criminal liabilities as stipulated under the Personal Data Protection Law. Data controllers—such as the Ministry of Health, hospitals, and digital health platforms—can be held accountable if they are found to process or disclose data belonging to medical personnel without a lawful basis or beyond the original purpose of collection. This regulation signifies that the state gives serious attention to protecting the data of medical personnel, as such violations not only breach legal norms but also threaten their physical and psychological safety as data subjects.

The practical implications become increasingly evident amid rapid digital health innovation, including the integration of electronic medical records, national platforms such as SatuSehat, and the expansion of telemedicine services. Without clear consent mechanisms and strict purpose-limitation controls, the data of medical personnel may easily migrate into secondary processing activities they never anticipated (Florea, 2023). Administrative data may be repurposed into performance analytics, reputation assessments, or even public exposure. Such uncertainty creates insecurity and resistance among medical personnel toward digital health initiatives.

Loss of control over personal data produces impacts that extend beyond legal concerns, as it directly affects the professional dignity of medical practitioners. When disciplinary histories, performance evaluations, or personal information are disclosed without proper consent, their professional reputation may be destroyed merely due to miscontextualized information. Even before ethical or legal processes conclude, medical personnel may experience social judgment far harsher than formal sanctions. This phenomenon clearly contradicts the presumption of innocence and procedural justice principles that should be upheld in a rule-based legal system.

The alleged sexual assault case involving an obstetrician identified as MSF in Garut exemplifies how the personal data of medical personnel can spiral out of

control in the absence of clear limits on data-processing purposes. Full identities, CCTV footage, and professional profiles were widely circulated across media platforms (Wulandari et al., 2025). Legally, the perpetrator may be held liable under the Sexual Violence Crime Law (UU TPKS), yet the uncontrolled public exposure illustrates the blurred boundaries between public interest and the privacy rights of the accused as a data subject. When the consent principle is disregarded, the evidentiary process can devolve into trial by media.

Similarly, the sexual assault case involving resident doctor PAP at RSHS Bandung demonstrates how malpractice, sexual violence, and hospital governance converge into a single issue. Beyond the criminal act itself, the case reveals how the personal data of medical personnel—including identity, education history, residency status, and professional records—can be exposed without limits (Ikaviola et al., 2025). This blurs the line between lawful law enforcement and public-driven social punishment. Without firm data protection guidelines, the public tends to assume that all information related to the perpetrator may be openly disclosed.

Data exposure risks increase further when the profiles of medical personnel—whether offenders or not—are integrated into national health platforms. Data such as registration numbers, practice locations, and training histories may leak or be cross-referenced with social media and news reporting. Without the application of privacy-by-design principles and clear consent for secondary processing, medical personnel may suffer compounded harm even when they are undergoing lawful legal procedures. At this point, the impacts on personal safety, psychological well-being, and professional standing become severe and unavoidable. Nonetheless, it must be acknowledged that in cases of sexual violence or serious misconduct, there is a legitimate public interest in revealing the perpetrator's identity to prevent recurrence of the crime. The challenge lies in balancing this public need with the consent principle and purpose-limitation requirements of the PDP Law.

Without firm guidelines, law-enforcement authorities and media outlets tend to treat all perpetrator-related data as fully public. Yet the PDP Law still requires data processing to remain proportional, relevant, and not excessive (Saly et al., 2023). Telemedicine research has shown that weak legal protection in remote healthcare services undermines the trust of both doctors and patients. Similar patterns appear in electronic medical records and professional platforms. When medical personnel feel that their data may be exploited without clear consent, they become reluctant to fully participate in reporting systems, research initiatives, or other data-driven innovations. As a result, data quality decreases, systemic learning from sexual violence or malpractice cases becomes obstructed, and the overall quality of healthcare services is adversely affected.

From a legal perspective, neglecting the consent principle opens the possibility of disputes across multiple domains. Administrative disputes may arise when medical personnel object to the display or publication of their profiles in national systems without adequate consent. Civil disputes may occur when reputational damage, loss of career opportunities, or threats to personal safety result from data leakage. In addition, ethical or disciplinary disputes may emerge if professional organizations deem institutional data management practices to be

inconsistent with professional codes of ethics. Without a clear consent framework, all these potential disputes fall into a legal grey area.

In practice, implementing the consent principle should not be seen as a barrier to public interest or digital health innovation. Through a consent-plus model that combines privacy-by-design principles, role-based access control, access-log recording, and data de-identification, the state can still utilize medical data for research and service evaluation without compromising the dignity of medical personnel. Through this approach, the public may still receive relevant information—such as sanctions against a doctor—without exposing irrelevant personal data (Utomo et al., 2020). Concrete steps such as clarifying consent clauses in employment contracts and privacy policies, separating consent for mandatory processing from secondary processing, and providing mechanisms for medical personnel to correct or refuse data processing can strengthen the implementation of the consent principle. Involving professional associations in establishing standards for the protection of medical personnel data can also ensure that the consent principle not only functions as a legal norm but becomes an institutional practice across the entire digital health system.

## Practical Consequences for Medical Personnel in the Context of Data Integration and Public Information Exposure

Data integration in modern health systems has fundamentally transformed the way information is managed and disseminated, and this shift brings direct implications for the professional lives of medical personnel. In an era when every clinical action, service record, and performance metric is stored in unified databases, medical workers face new conditions that demand rapid adaptation. What was once recorded manually and confined to internal administrative spaces is now embedded in vast networks connecting institutions, agencies, and even the public through digital health platforms (Putri, 2025). This situation not only expands the accessibility of information but also increases the potential for data misuse or misinterpretation by parties outside the medical profession. These dynamics create practical consequences that cannot be overlooked, as they affect personal security, professional responsibility, relationships with patients, and the psychological well-being of medical personnel.

One of the most immediate consequences is the heightened transparency of medical personnel's work records, which automatically activates stricter and more continuous audit mechanisms. Every clinical action—from diagnosis to minor procedures—can now be traced with high precision. On one hand, this mechanism may improve service quality and minimize malpractice, but on the other hand, medical personnel must confront psychological pressure stemming from the feeling of constant surveillance, even in complex clinical situations. Digital systems often present data in the form of dry statistics—service duration, number of patients handled, or procedural compliance scores—which fail to reflect the full context or nuances of the cases encountered. This consequence leads some practitioners to adopt more defensive approaches when making clinical decisions, not solely for patient health considerations but due to concerns that their data will be negatively evaluated.

Beyond audit pressure, data integration increases the vulnerability of medical personnel to personal information leaks. Data such as identity, practice address, registration numbers, or even certain private details are frequently stored in systems that are not entirely secure against cyberattacks. As cyber threats continue to rise, medical personnel become attractive targets because their information holds significant value to malicious actors (Herdadi, 2024). Data breaches not only damage reputations but also create risks of physical threats such as intimidation or identity misuse. In several cases across different countries, medical personnel have even faced direct attacks from individuals exploiting digital information for criminal purposes, turning data security issues into urgent matters of personal safety.

Another consequence emerges in the interaction between medical personnel and the public, especially due to the increased exposure of information through digital health platforms that provide ratings, reviews, and performance metrics. The public can now access information about doctors or healthcare workers through applications or official health service websites. While some of this information is intended to foster transparency and public trust, not all data is interpreted proportionally. Public evaluations often contain emotional bias or personal experiences that do not always reflect objective clinical competence. As a result, medical personnel may suffer unjust reputational pressure even when they have acted in accordance with professional standards.

Data integration also influences clinical decision-making patterns. Because all actions are recorded and potentially reviewable by the public or oversight bodies, medical personnel may feel compelled to choose decisions that appear "safe" from the perspective of statistics and digital evaluation rather than based on a more comprehensive medical assessment. For instance, they may prefer standard procedures over alternative approaches that are clinically appropriate but statistically riskier (Manurung & Simarmata, 2025). This phenomenon is known as data-driven defensive medicine, which in the long term may hinder clinical innovation and reduce the flexibility of medical workers to adjust decisions according to each patient's unique context. Indirectly, data integration shifts the orientation of medical practice from professional integrity to fear-driven digital scrutiny.

Another practical consequence concerns the increasing administrative burden placed on medical personnel. With the adoption of electronic medical records, digital input applications, and mandatory digital reporting, medical workers must develop substantial digital literacy. They must manage accounts, protect passwords, follow encryption protocols, and ensure compliance with personal data protection regulations. This additional burden reduces the time that should be spent interacting with patients or performing clinical analysis. Many medical personnel report high levels of fatigue due to heightened administrative pressure—a condition known in international literature as digital burnout.

Changes also emerge in the dynamics of therapeutic relationships between medical personnel and patients. As patients gain access to various information about their healthcare providers—whether from official or unofficial sources—they enter clinical encounters with certain expectations that may strengthen or disrupt trust. In some cases, such exposure reassures patients because they feel

familiar with the credibility of the medical personnel treating them (Hanifah & Irawati, 2024). In other situations, negative or subjective reviews may create prejudice that complicates therapeutic communication. Medical personnel must work harder to rebuild trust that has been distorted by digital exposure.

Data integration also introduces practical consequences in cross-institutional collaboration. Information about medical personnel now circulates among hospitals, the Social Security Agency (BPJS), the Ministry of Health, regional health offices, and technology companies providing digital health platforms. Each entity uses different security standards, interests, and data processing mechanisms, meaning that medical personnel become part of a complex digital bureaucracy. Errors in data input, incompatible security standards, or interpretative discrepancies between institutions may generate administrative or reputational problems. Medical personnel may be blamed even when the issue originates from systemic weaknesses rather than from their actions.

In the context of big-data-based health research, medical personnel often serve as sources of data for studies conducted by hospitals or academic institutions. Although such research offers major benefits, medical personnel frequently lack control over how their data is used. Sometimes data is processed using analytic methods that produce conclusions about their performance without giving them the opportunity to clarify or contextualize the findings (Supriyadi, 2023). In such scenarios, medical personnel become objects of data rather than subjects participating in its governance. Ethically, public information exposure and data integration place medical personnel in a dilemma. They are required to strictly protect patient privacy, yet their own privacy is often insufficiently protected. This asymmetry raises questions about digital justice in the health sector. How can medical personnel be expected to uphold rigorous personal data protection standards for patients while the system itself fails to provide equivalent protection for their own data? This imbalance gradually affects motivation, workplace comfort, and overall service quality.

## Conclusion

The principle of consent in the protection of medical personnel's personal data serves as an ethical and legal foundation ensuring that every form of data collection, processing, and distribution involving medical workers is carried out knowingly, voluntarily, and with full understanding by the individuals concerned. This principle affirms that medical personnel have the right to know the purposes for which their data is used, the limitations of access, and the parties authorized to manage it. In the context of modern healthcare, characterized by digitalization and integrated information systems, the principle of consent becomes a crucial instrument for maintaining balance between the need for data to enhance healthcare services and the individual rights of medical personnel to privacy, security, and control over their personal information.

The implications and consequences of implementing—or neglecting—the consent principle significantly determine the quality of legal protection and professional well-being of medical personnel in the digital era. When this principle is applied consistently, medical personnel are protected from risks such as data

breaches, misuse of information, reputational pressure, and disproportionate administrative burdens. Conversely, when consent is ignored or weakly enforced, medical personnel may face serious vulnerabilities in legal, ethical, and psychological dimensions due to uncontrolled public exposure of information and cross-institutional data integration that remains insufficiently secure. Therefore, strengthening the consent principle is not merely a technical requirement but a normative imperative to ensure that digital transformation in the healthcare sector proceeds fairly, proportionately, and with full respect for the dignity of the profession.

## References


Benuf, K., & Azhar, M. (2020). Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. *Gema Keadilan*, *7*(1), 20–33.

Damayanti, P. S., Adiputra, I. M. S., & Pradnyantara, I. G. A. N. P. (2025). Tantangan penerapan Rekam Medis Elektronik (RME) berdasarkan regulasi Permenkes No. 24 Tahun 2022. *Health Sciences and Pharmacy Journal*, *9*(1), 47–55. https://doi.org/10.32504/hspj.v9i1.1164

Fahmanadie, D., Sukmawan, Y., Ifrani, I., Topan, M., Abdullah, D., Amrin, M. A., Barakatullah, A. H., Syafrilla, R. J., & Wardani, D. K. (2025). Optimalisasi Pemahaman Hukum Tenaga Medis dan Tenaga Kesehatan dalam Perlindungan Data Pribadi Pasien di Rumah Sakit. *KREATIF: Jurnal Pengabdian Masyarakat Nusantara*, *5*(4), 257–267. https://doi.org/10.55606/kreatif.v5i4.8487

Florea, M. (2023). Withdrawal of Consent for Processing Personal Data in Biomedical Research. *International Data Privacy Law*, *13*(2), 107–123. https://doi.org/10.1093/idpl/ipad008

Frederico, L., Batubara, S. A., & Pakpahan, E. F. (2024). Perlindungan Hukum terhadap Data Pasien sebagai Jaminan atas Data Pribadi dalam Pelayanan Kesehatan. *Unes Journal of Swara Justisia*, *8*(2), 379–386. https://doi.org/10.31933/2ybkxb89

Guamo, I. (2025). Analisis Keterbatasan Regulasi Sanksi Malpraktik Tenaga Medis Asing dan Konsekuensinya Terhadap Penegakan Hukum di Indonesia. *Jurnal Hukum Caraka Justitia*, *5*(2), 198–209. https://doi.org/10.30588/jhcj.v5i2.2215

Hanifah, H. N., & Irawati, A. C. (2024). Urgensi Cyber Law dalam Menjaga Privasi Pasien di Rumah Sakit Era Digital. *ADIL Indonesia Journal*, *5*(2), 154–161. https://doi.org/10.35473/aij.v5i2.3945

Herdadi, A. (2024). Analisis Keamanan Siber pada Implementasi Sistem Informasi Rekam Medis Openemr V7.0.2. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *7*(4), 824–833. https://doi.org/10.32672/jnkti.v7i4.7887

Herisasono, A. (2024). Perlindungan Hukum terhadap Privasi Data Pasien dalam Sistem Rekam Medis Elektronik. *Jurnal Kolaboratif Sains*, *7*(12), 4677–4681. https://doi.org/10.56338/jks.v7i12.6620

Ikaviola, F. I. D., Noviridah, S. N., Lestari, C. A., Meisyah, I., Febriantsyah, M. S., & Suryaningsi, S. (2025). Ketika Kepercayaan Publik Diuji: Refleksi Kritis Atas

Kasus Kekerasan Seksual Oleh Dokter Residen. *Causa: Jurnal Hukum Dan Kewarganegaraan*, *14*(7), 11–20. https://doi.org/10.6679/b93thq71
julsandri. (2025). Legal Aspects of Protecting Patient Medical Data in The e-Puskesmas System. *Juridica: Jurnal Fakultas Hukum Universitas Gunung Rinjani*, *7*(1), 27–39. https://doi.org/10.53952/juridicaugr.v7i1.462
Manurung, P. I. R., & Simarmata, M. (2025). Digitalisasi Layanan Kesehatan: Tantangan Etika dan Keamanan Data Pasien. *Presidensial: Jurnal Hukum, Administrasi Negara, Dan Kebijakan Publik*, *2*(2), 263–273. https://doi.org/10.62383/presidensial.v2i2.811
Punia, I. G. E. A. A. (2025). Aspek Bioetika Penyimpanan Data dalam Rekam Medis Elektronik. *Jurnal Etika Kedokteran Indonesia*, *9*(3). https://ilmiahindonesia.id/index.php/jeki/article/view/49
Putri, H. A. (2025). Legal Review of the use of Personal Data in the Development of Artificial Intelligence Under the Personal Data Protection Law. *Jentera: Jurnal Hukum*, *6*(1), 1–15.
Rizqiyanto, N., Rohman, A. F., & Raya, F. A.-H. M. (2024). Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Media Hukum Indonesia (MHI)*, *2*(2), 1–14. https://doi.org/10.5281/zenodo.10995150
Rosadi, S. D. (2017). Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit menurut Ketentuan Nasional dan Implementasinya. *Sosiohumaniora*, *19*(3), 206–212. https://doi.org/10.24198/sosiohumaniora.v19i3.11380
Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023). Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022. *Jurnal Serina Sosial Humaniora*, *1*(3), 145–153.
Siregar, R. A. (2024). Penerapan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis terhadap Efektivitas Pelayanan Kesehatan. *JIHK*, *5*(2), 1–15. https://doi.org/10.46924/jihk.v5i2.182
Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*, *3*(1), 33–69. https://doi.org/10.53955/jhcls.v3i1.71
Swede, M. J., Scovetta, V., & Eugene-Colin, M. (2019). Protecting Patient Data Is the New Scope of Practice: A Recommended Cybersecurity Curricula for Healthcare Students to Prepare for this Challenge. *Journal of Allied Health*, *48*(2), 148–156.
Sylviana, G., Maharani, D. P., & Wibowo, A. M. (2025). Keabsahan Praktik Dark Patterns Terhadap Pemerolehan Persetujuan Pemrosesan Data Pribadi di Indonesia. *RechtJiva*, *2*(1), 66–85. https://doi.org/10.21776/rechtjiva.v2n1.5
Utomo, H. P., Gultom, E., & Afriana, A. (2020). Urgensi Perlindungan Hukum Data Pribadi Pasien dalam Pelayanan Kesehatan Berbasis Teknologi di Indonesia. *Jurnal Ilmiah Galuh Justisi*, *8*(2), 168–185. https://doi.org/10.25157/justisi.v8i2.3479
Winkler, E. C., Jungkunz, M., Thorogood, A., Lotz, V., & Schickhardt, C. (2025). Patient data for commercial companies? An ethical framework for sharing patients' data with for-profit companies for research. *Journal of Medical Ethics*, *51*(5). https://doi.org/10.1136/jme-2022-108781

Wulandari, R. A., Kamal, L. F., Tobing, F. O., Sinamo, S. N., Narendra, A. C., & Suryaningsi, S. (2025). Etika Medis dan Pancasila: Telaah Kasus Kekerasan Seksual Garut. *Sindoro: Cendikia Pendidikan*, *16*(4), 31–40. https://doi.org/10.99534/aknn6076