DOI: 10.46924/jihk.v7i2.381

The Construction of the Consent Principle in the Protection of Medical Personnel's Personal Data and Its Legal Consequences in Healthcare Practice

Juan Ponce Enrile Febriansyah[1]* & Ida Kurnia[2]

[1,2]Faculty of Law, Universitas Tarumanagara Jakarta, Indonesia

Correspondence

Juan Ponce Enrile Febriansyah, Faculty of Law, Universitas Tarumanagara Jakarta, Indonesia, Letjen S. Parman St No.1, RT.6/RW.16, Tomang, Grogol petamburan, West Jakarta City, Jakarta 11440, *e*-mail: enrilefebriansyah2@gmail.com

How to cite

Febriansyah, Juan Ponce Enrile., & Kurnia, Ida. 2026. The Construction of the Consent Principle in the Protection of Medical Personnel's Personal Data and Its Legal Consequences in Healthcare Practice. *Jurnal Ilmu Hukum Kyadiren*. *7*(2), 1181-1196. https://doi.org/10.46924/jihk.v7i2.381

Original Article

Abstract

This study analyzes the implementation of the consent principle in the protection of personal data of healthcare workers in Indonesia, focusing on its implications and consequences in the context of digital healthcare services. As digital transformation accelerates in the healthcare sector, with the adoption of electronic medical records, telemedicine, and health applications, the personal data of healthcare workers, including doctors and nurses, is increasingly exposed and at risk of misuse. According to Law No. 27 of 2022 on Personal Data Protection (UU PDP), the consent principle is the primary basis for legitimate data processing. However, this research reveals a gap between existing regulations and their implementation, which could lead to legal, ethical, and professional consequences for healthcare workers. Findings indicate that, despite the normative regulation of consent in the UU PDP, its application in digital health policies remains weak and inconsistent. This study suggests the need for regulatory improvements and stronger enforcement of the consent principle to effectively protect the personal data of healthcare workers.

Keywords: *Consent Principle, Personal Data Protection, Healthcare Workers, Legal Implications, Digital Health*

Abstrak

Penelitian ini menganalisis penerapan prinsip persetujuan dalam perlindungan data pribadi tenaga medis di Indonesia, dengan fokus pada implikasi dan konsekuensinya dalam hal layanan kesehatan digital. Seiring dengan transformasi digital dalam sektor kesehatan, seperti penerapan rekam medis elektronik, telemedisin, dan aplikasi kesehatan, data pribadi tenaga medis, termasuk dokter dan perawat, semakin terpapar dan berisiko disalahgunakan. Berdasarkan Undang-Undang Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022, prinsip persetujuan menjadi dasar yang sah dalam pemrosesan data pribadi. Namun, penelitian ini mengungkapkan adanya kesenjangan antara regulasi yang ada dan implementasinya, yang berpotensi menimbulkan konsekuensi hukum, etik, dan profesional bagi tenaga medis. Temuan menunjukkan bahwa meskipun prinsip persetujuan diatur secara normatif dalam UU PDP, penerapannya dalam kebijakan kesehatan digital masih lemah dan tidak konsisten. Penelitian ini menyarankan perlunya perbaikan regulasi dan penguatan implementasi prinsip persetujuan yang lebih tegas untuk melindungi data pribadi tenaga medis secara efektif.

Kata Kunci: *Prinsip Persetujuan, Perlindungan Data Pribadi, Tenaga Medis, Implikasi Hukum, Kesehatan Digital*

1. INTRODUCTION

The digital transformation of healthcare services in Indonesia—including the adoption of electronic medical records, telemedicine, health applications, and big health data systems—has expanded the collection and processing of personal data not only for patients but also for healthcare professionals, particularly physicians and nurses. Their personal data encompass identity information, STR and SIP numbers, educational background, performance records, practice schedules, and disciplinary histories, all of which are legally recognized as protected personal data.[1] However, normative and empirical research has largely centered on patient data protection, while the personal data of medical personnel have received comparatively little attention.[2] This gap highlights a disconnect between the evolution of personal data protection regulations and the actual safeguards provided to healthcare professionals as data subjects.[3]

Law No. 27 of 2022 on Personal Data Protection designates consent as a primary legal basis for processing personal data, requiring it to be explicit, specific, and informed. For doctors and nurses, their data are processed by various entities—hospitals, clinics, insurance providers, and digital health platforms—for administrative functions, credentialing, performance evaluation, service quality monitoring, and commercial partnerships. Masidin notes that data protection frameworks in the health sector remain predominantly sectoral and insufficiently aligned with the general principles of the PDP Law, including the foundational requirement of consent. In this regard, the concept of privacy by design is essential for healthcare application development, mandating that consent mechanisms be embedded at the system design stage rather than treated as a procedural formality.[4]

Institutional and legal preparedness within healthcare facilities significantly shapes the effectiveness of applying the consent principle to medical personnel. Siregar and Astuti found that many healthcare workers in Indonesia, including physicians and nurses, lack adequate understanding of personal data protection principles and rely more heavily on professional ethics than on formal regulatory compliance.[5] This is reflected in unclear internal policies regarding their rights to information and consent in data processing, such as the use of performance metrics for managerial or promotional purposes. Consequently,

---

1 Rospita Adelina Siregar dan Nanin Koeswidi Astuti, "Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia," *International Journal of Law, Policy and Social Review* 7, no. 3 (2025): 15–21, https://www.lawjournals.net/archives/2025/7/3/7062.

2 Alfian Listya Kurniawan dan Anang Setiawan, "Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19," *Jurnal Hukum dan Pembangunan Ekonomi* 9, no. 1 (2021): 95–112, https://doi.org/10.20961/hpe.v9i1.52586.

3 Masidin, "Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Jurnal Hukum: Officium Nobile* 1, no. 1 (2024): 1–12, https://journal.unas.ac.id/jhon/article/view/3866.

4 Vermonita Dwi Caturjayanti, "Konsep Privacy by Design sebagai Perlindungan Data Pribadi Pengguna Aplikasi 'Peduli Lindungi,'" *Rewang Rancang: Jurnal Hukum Lex Generalis* 1, no. 9 (2020): 70–87, https://doi.org/10.56370/jhlg.v1i9.251.

5 Siregar dan Astuti, "Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia."

consent is often broad or implied, without sufficient explanation of its purpose, duration, or data recipients.

The rapid expansion of digital health innovations further complicates the issue. With telemedicine and electronic medical records, regulatory fragmentation and overlapping legal provisions create uncertainty concerning data control, the procedures for obtaining consent from doctors and nurses, and the permissible scope of data processing and third-party sharing.[6] In practice, many healthcare professionals join digital platforms or hospital information systems by signing membership or employment agreements containing general data protection clauses, with limited opportunity to understand or negotiate their consent as data subjects.[7]

The adoption of electronic medical records illustrates how the personal data of physicians and nurses are closely integrated into digital infrastructures. Although electronic medical records enhance the security and efficiency of information management, they continue to encounter challenges regarding their recognition as legal evidence and compliance with normative requirements.[8] Within the same system, physicians' and nurses' clinical activities—including treatment notes, clinical assessments, and work patterns—are recorded in detail and may be processed for additional purposes such as performance evaluations or internal audits.[9] Without explicit and informed consent, secondary use of these data risks exceeding the original purpose of collection and may generate legal and ethical implications.

Debates surrounding consent in Indonesian health law have primarily addressed informed consent for medical procedures. Its implementation continues to face challenges stemming from disparities in understanding and language between healthcare personnel and patients.[10] In emergency situations, informed consent functions as a legal safeguard for healthcare providers, although patients' comprehension of the procedures explained often remains limited.[11] In regions with low health literacy, the practice of informed consent tends to be formalistic and does not fully represent conscious and voluntary

---

6 Gunawan Widjaja et al., "Perlindungan Hukum Bagi Pasien dan Tenaga Medis Dalam Inovasi Kesehatan Digital: Tinjauan Literatur Terhadap Peraturan Perundang-Undangan di Indonesia," *JK: Jurnal Kesehatan* 3, no. 2 (2025): 200–210, https://wikep.net/index.php/JUKESAH/article/view/268/242.

7 Widjaja et al.

8 Ichsan Anwary dan Rusma Wahyudi, "Perlindungan Hukum Terhadap Dokter, Dokter Gigi dan Pasien Pada Penerapan Rekam Medis Elektronik di Rumah Sakit," *Badamai Law Journal* 6, no. 1 (2021): 150–69, https://doi.org/10.32801/damai.v6i1.11755.

9 I Wayan Dody Putra Wardana et al., "Legal Protection for Medical Recorders and Health Information Personnel in the Management of Electronic Medical Records," in *Procedia of Engineering and Life Science Universitas Muhammadiyah Sidoarjo* (Sidoarjo: Universitas Muhammadiyah Sidoarjo, 2025), https://doi.org/10.21070/pels.v7i0.2091.

10 Erlen Enjelita Kikhau, Rudepel Petrus Leo, dan Debi F.Ng Fallo, "Pelaksanaan Persetujuan Tindakan Medis (Informed Consent) Sebagai Upaya Perlindungan Hukum Bagi Tenaga Medis dan Pasien," *Jurnal Hukum Bisnis* 12, no. 6 (2023): 1–10, https://doi.org/10.47709/jhb.v12i06.3073.

11 Winarti dan Rizka, "Informed Consent sebagai Upaya Perlindungan Hukum Bagi Tenaga Kesehatan dalam Kasus Medis Darurat (Studi Kasus di Rumah Sakit Umum Daerah Provinsi Papua Barat)," *Sehat Rakyat Jurnal Kesehatan Masyarakat* 4, no. 2 (2025): 264–77, https://doi.org/10.54259/sehatrakyat.v4i2.4310.

agreement.[12] While issues in informed consent persist even for long-established medical procedures, the challenges of applying consent to personal data processing, including that of physicians and nurses, are becoming increasingly complex.

Work relationships and organizational hierarchies within healthcare institutions also shape the quality of medical personnel's consent to the processing of their personal data. While health ethics and law emphasize respect for the professional autonomy of healthcare workers, administrative decisions in practice are frequently driven by institutional priorities.[13] Legal protection for nurses extends beyond safeguarding against malpractice through clear communication and written documentation; it also involves ensuring legal certainty in the exercise of their profession.[14] When nursing documentation and performance evaluations are disclosed or shared without proper consent, they may affect professional reputation, career advancement, and the sense of security in performing clinical duties. Similar concerns apply to physicians, whose data may be used for profiling, heightened surveillance, or unilateral assessments by management or third parties.

From a data governance standpoint, the role of medical recorders and health information officers is particularly strategic because they manage and access both patient data and healthcare worker data.[15] These personnel require clear legal safeguards, as errors in data handling may carry ethical, administrative, and civil consequences. If the procedures and legal foundations for processing the personal data of medical personnel—especially the principle of consent—are not explicitly regulated, the likelihood of processing errors or misuse of physician and nurse data increases. Consequently, weaknesses in consent mechanisms not only disadvantage patients but also place doctors, nurses, and medical record staff within a shared environment of vulnerability.

These conditions carry significant implications and consequences due to the weak application of the consent principle in protecting the personal data of physicians and nurses. Legally, data processing conducted without valid consent may be categorized as a violation of the PDP Law and sectoral health regulations, potentially resulting in administrative sanctions, civil liability, and criminal penalties for data controllers and processors.[16] Ethically and professionally, the disclosure or misuse of medical personnel's personal data can harm reputations, create stigma, and lead to unfair performance evaluations. Institutionally, the absence of a transparent consent mechanism can erode the

---

12 Gusti Ayu Made Purnama Dewi dan I Putu Gede Adiatmika, "Legal and Ethical Analysis of the Implementation of Informed Consent in Medical Practice in Indonesia," *Babali Nursing Research* 6, no. 3 (2025): 578–85, https://doi.org/10.37363/bnr.2025.63491.

13 Muhamamad Is Sadi, *Etika dan Hukum Kesehatan* (Jakarta: Kencana, 2010), hal. 190.

14 R. H. Riasari, "Perlindungan Hukum terhadap Perawat pada Rumah Sakit Berdasarkan Undang-Undang Nomor 38 Tahun 2014 tentang Keperawatan," *Rewang Rancang: Jurnal Hukum Lex Generalis* 2, no. 10 (2021): 946–60, https://doi.org/10.56370/jhlg.v2i10.79.

15 Cahyadi Ramadhani, Nayla Alwiya, dan Ulil Afwa, "Perlindungan Hukum Perekam Medis Dalam Pelayanan Rekam Medis dan Informasi Kesehatan di Fasilitas Pelayanan Kesehatan," *Soedirman Law Review* 3, no. 2 (2021): 1–12, https://doi.org/10.20884/1.slr.2021.3.2.149.

16 Masidin, "Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

trust of doctors and nurses in healthcare organizations and digital platforms, ultimately hindering the sustainability of digital health innovations that depend on their active participation.

Government policy case studies during the pandemic—particularly those concerning the determination of pandemic status and vaccination programs—serve as important reference points for reassessing the consent principle in health-sector data processing. Although the policies primarily addressed public health considerations, their substance and corresponding legal debates implicate the protection of citizens' constitutional rights to privacy and control over personal data. This aligns with the PDP Law, which requires all personal data processing, including health data and medical personnel profiles, to be grounded in valid consent, implemented transparently, and guided by the principles of privacy by design and privacy by default. Accordingly, various digital health policies, including data integration under Ministerial Regulation 24/2022 and platforms such as SatuSehat, must be evaluated to determine whether they genuinely uphold the rights of doctors and nurses as data subjects rather than merely positioning them as administrative instruments within public policy frameworks.[17]

The case of sexual harassment involving a gynecologist identified as MSF in Garut illustrates how the public disclosure of a healthcare professional's identity and professional history can directly conflict with the consent principle in personal data protection. The widespread circulation of CCTV footage on social media, together with extensive reporting on the perpetrator's initials, practice location, and educational background, shows that once a criminal case involving medical personnel emerges, the boundary between the public's right to information and the perpetrator's right to privacy often becomes indistinct. On one hand, revealing the doctor's identity serves an important role in encouraging additional victims to come forward, creating a deterrent effect, and reinforcing professional accountability. On the other hand, when information shared surpasses what is necessary for law enforcement for instance, by distributing detailed biographical data, home addresses, or administrative information sourced from hospital systems or healthcare platforms without consent and without a clear legal basis such disclosure risks violating the PDP Law's principles of purpose limitation and data minimization. It also establishes a problematic precedent for safeguarding the personal data of physicians and other healthcare workers who are not involved in the case but may nonetheless experience institutional stigma.

Similarly, the repeated sexual assault case involving a PAP resident doctor at RSHS Bandung demonstrates that the issue extends beyond ethical and criminal dimensions and also concerns the management of personal data belonging to medical personnel.[18] Throughout the case proceedings, various authorities and media outlets disclosed multiple

[17] Caturjayanti, "Konsep Privacy by Design sebagai Perlindungan Data Pribadi Pengguna Aplikasi 'Peduli Lindungi.'"

[18] Tempo, "Kronologi Pemerkosaan 2 Korban Baru Dokter Priguna," Tempo.co.id, 2025, https://www.tempo.co/hukum/kronologi-pemerkosaan-2-korban-baru-dokter-priguna-1230771.

pieces of information about the perpetrator, including full name, residency status, educational affiliation, and administrative sanctions such as the revocation of the STR and SIP. From a personal data protection standpoint, these disclosures must be evaluated against the standards set by the PDP Law: determining which data qualify as "mandatory disclosure" in the interest of justice and crime prevention, and which data should remain restricted for use solely in law enforcement and professional discipline. Moreover, hospital and medical campus information systems contain not only perpetrator data but also work schedules, resident rosters, nurse team information, and other sensitive data, the exposure of which could endanger the safety and reputation of healthcare workers who are not involved in the incident. This situation underscores the importance of implementing privacy by design and establishing clear consent mechanisms for the use of medical personnel's profile data, even when they are implicated or suspected of involvement in criminal cases.

If digital health policies are not accompanied by firm and proportionate regulations governing the management of medical personnel's personal data, the cases in Garut and RSHS Bandung illustrate the potential consequences. On one hand, the state and healthcare institutions have an obligation to ensure full accountability for perpetrators of sexual violence, protect victims, and maintain public trust through adequate information disclosure. On the other hand, the PDP Law and the consent principle emphasize that even in criminal cases, personal data management must not amount to an unrestricted takeover of an individual's profile, nor allow open access to data irrelevant to law enforcement purposes. For physicians and nurses as the backbone of healthcare services, ensuring that their personal data are processed only as necessary, based on valid consent and safeguarded by strict technical and organizational measures, constitutes an essential aspect of their professional rights. Therefore, the integration of electronic health systems under Ministerial Regulation 24/2022—including SatuSehat and hospital electronic medical record platforms—must be reassessed to ensure that perpetrators are not shielded, victims remain protected, and the personal data rights of doctors and nurses are upheld through transparent, accountable, and mutually agreed-upon policies and procedures.[19]

Based on the preceding discussion, it is evident that the principle of consent forms a central foundation for safeguarding the personal data of medical personnel, particularly physicians and nurses, amid the rapid digitalization of healthcare services. Although a normative framework has been established through the PDP Law and various health-sector regulations, the actual practices of data processing within healthcare institutions and digital platforms frequently diverge from these legal requirements. This misalignment generates concerns that extend beyond legal dimensions and implicate ethical and

[19] Elfian Fauzy dan Nabila Alif Radika Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Lex Renaissance* 7, no. 3 (2023): 445–61, https://doi.org/10.20885/JLR.vol7.iss3.art1.

professional issues, as medical personnel face heightened vulnerability when their personal data are processed without a clear and valid basis for consent.

This context underscores the necessity of the present study. Under the title "The Principle of Consent in the Protection of Personal Data of Medical Personnel: Implications and Consequences," the research examines how the consent principle is articulated and applied, as well as the challenges that arise when it is fulfilled only in a formalistic manner or disregarded entirely. Accordingly, the study focuses on two primary questions: first, how the regulatory framework and practical implementation of the consent principle for the protection of medical personnel's personal data are structured under the PDP Law and relevant sectoral regulations—particularly Minister of Health Regulation No. 24 of 2022—in the context of digital health innovation; and second, what legal and practical implications emerge from the implementation or non-implementation of this principle in the operation of digital healthcare services.

2. RESEARCH METHODOLOGY

This thesis employs a normative juridical research method with an analytical–descriptive orientation. Normative juridical research is carried out through library-based inquiry focused on examining primary, secondary, and tertiary legal materials.[20] Primary legal materials include the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, Law No. 36 of 2009 on Health, Law No. 29 of 2004 on Medical Practice, Minister of Health Regulation No. 24 of 2022 on Medical Records, and other relevant statutes and regulations governing the health sector and the medical profession. Secondary materials consist of books, journals, research reports, and legal commentaries, while tertiary materials encompass legal dictionaries, encyclopedias, and indexes.[21] Document study serves as the primary data collection technique, involving a systematic review of statutory provisions, court decisions, and legal scholarship to assess the consistency, relevance, and application of legal norms relating to the protection of medical personnel's personal data. Within this methodological framework, the research not only outlines existing legal norms but also evaluates the positioning of informed consent and approval under the PDP Law in relation to the legal protection afforded to doctors and nurses.

The study employs three complementary legal approaches: the statute approach, the case approach, and the conceptual approach.[22] The statute approach involves examining the PDP Law, the Health Law, the Medical Practice Law, Minister of Health Regulation No. 24 of 2022, and related implementing regulations governing medical records and the protection of medical personnel's personal data. The case approach is applied by reviewing

---

[20] Soerjono Soekanto, *Pengantar Penelitian Hukum* (Jakarta: UII Press, 2012), hal. 25.

[21] Gary Chan Kok Yew dan Michael Yip, *Data and Private Law: Translating Theory into Practice* (Oxford: Hart Publishing, 2021), hal. 120.

[22] Sugiyono, *Metode Penelitian Kualitatif* (Bandung: Rake Sarasin, 2020), hal. 80.

pertinent cases, including data breaches, public disclosure of medical personnel profiles, and incidents of sexual violence by medical personnel that resulted in the exposure of their personal data, to assess how the principles of consent and personal data protection are adhered to—or neglected—in practice. The conceptual approach is used to clarify essential concepts such as medical personnel, personal data protection, privacy, and informed consent. All collected data are analyzed descriptively and qualitatively using deductive reasoning, beginning with general legal principles and norms and applying them to the specific cases examined. Through this method, the research aims not only to describe the content of legal provisions but also to evaluate their practical application to the protection of medical personnel's personal data.[23]

3. RESULT AND DISCUSSION

3.1. Regulatory Framework and Implementation of the Consent Principle in Protecting the Personal Data of Medical Personnel

Normatively, Law No. 27 of 2022 on Personal Data Protection (PDP Law) establishes consent as one of the legal bases for processing personal data. The PDP Law defines personal data as information relating to an identified or identifiable individual and explicitly recognizes "specific personal data," which includes health data. Within this framework, data belonging to physicians and nurses—such as personal and professional identifiers, registration numbers (STR/SIP), educational history, disciplinary records, and even their own health information—constitute personal data subject to the principles of lawfulness, purpose limitation, data minimization, accuracy, and security set out in the PDP Law. Medical personnel therefore occupy a dual position: they are data subjects whose privacy must be protected, while simultaneously serving as parties who process patient data in the course of their professional duties.

The PDP Law requires that all personal data processing must rely on a valid legal basis. For specific personal data, such as health information, the primary basis is the data subject's explicit consent, unless otherwise provided by law—for instance, in situations involving the public interest in the health sector, compliance with state legal obligations, or law enforcement. As a result, processing the personal data of physicians and nurses by hospitals, the Ministry of Health, professional organizations, and digital health platforms should be grounded in clear information regarding the purpose of collection, the nature of the data processed, the retention period, the applicable legal basis, and any potential sharing with third parties. Beyond core employment or professional functions—such as internal credentialing—secondary uses, including displaying profiles on public platforms or utilizing data for research or analytics, should adhere to the requirement of free, specific, and informed consent.

---

[23] Soekanto, *Pengantar Penelitian Hukum*, hal. 101.

Within the health law framework, Law No. 36 of 2009 on Health and Law No. 29 of 2004 on Medical Practice recognize the principles of medical confidentiality and the right to privacy. Physicians and nurses are obligated to maintain the confidentiality of information obtained in relation to their patients, and breaches of this duty may result in ethical, administrative, civil, or criminal sanctions. However, these legal norms focus more heavily on protecting patient data. The position of medical personnel as holders of personal data is not comprehensively regulated, particularly with respect to how their profile information, performance records, and professional data may be processed, stored, integrated, or disclosed within the national digital health ecosystem. This regulatory gap raises important questions about the extent to which the consent principle under the PDP Law is effectively operationalized to protect physicians and nurses.

Minister of Health Regulation No. 24 of 2022 on Medical Records serves as a key technical regulation governing the digitization and integration of electronic medical records through national platforms such as SatuSehat. The regulation requires healthcare facilities to input, store, and transmit medical records into a centralized system, which also contains the identities of the medical personnel who provide care. In practice, this results in physician and nurse profiles—including names, registration numbers, specialties, and other professional attributes—being incorporated into the national system. The legal basis for this processing rests on statutory obligations imposed on the state and healthcare facilities, rather than on the individualized consent of medical personnel.

From the perspective of the PDP Law, reliance on "exercise of state authority" or "public interest" may substitute for consent as a legal basis but does not exempt data controllers from adhering to general personal data protection principles. The Ministry of Health and healthcare facilities function as Data Controllers and/or Data Processors and must uphold purpose limitation, transparency, security, and accountability. Normatively, clear rules should delineate: (a) the scope of personal data collected and integrated from medical personnel; (b) who may access such data, both internally and externally; (c) the purposes for which medical personnel profiles may be displayed publicly; and (d) the mechanisms for objection, correction, and deletion when a doctor or nurse believes their privacy rights have been infringed.

At the technical regulatory level, Minister of Health Regulation No. 24/2022 prioritizes mandatory data integration and procedures for maintaining electronic medical records rather than specifying consent mechanisms for medical personnel as data subjects. The regulation does not explicitly address, for instance, whether medical personnel have the right to consent to or decline the use of their profiles for purposes beyond direct service, nor does it establish procedures for restricting the public display of certain data. As a result, although the PDP Law formally recognizes the importance of consent, its application to medical personnel's personal data tends to be absorbed under the justification of public interest and state authority, leaving data subjects without meaningful control.

A more progressive model for regulating consent is reflected in the concepts of privacy by design and privacy by default. These principles require that personal data protection—including the ability to grant or refuse consent—be embedded from the earliest stages of system design rather than appended at the administrative level. Applied to SatuSehat and electronic medical records, this approach demands the inclusion of a consent management module for medical personnel, granular settings governing which profile elements may be publicly displayed, and opt-in or opt-out mechanisms for data uses beyond direct care, such as research, performance profiling, or publication.

In practice, however, existing regulatory frameworks and technical system designs remain oriented toward efficiency and data integration, rather than strengthening the position of doctors and nurses as data subjects. There is no explicit privacy-by-design paradigm that frames medical personnel's consent as a form of self-determination. For example, no clear rules specify whether medical personnel may restrict access to certain disciplinary records or whether they have a right to be notified when their data are used for policy analytics, performance audits, or external research. These gaps illustrate the divergence between the normative commitments of the PDP Law and the sectoral regulations within the health system.

Research on telemedicine further underscores this point. Studies consistently indicate that Indonesia's regulatory structure for digital health services, particularly telemedicine, remains underdeveloped in terms of legal substance, institutional support, and legal culture. Telemedicine is considered high-risk yet is governed by limited protections, many of which emerged during the pandemic and have not been formalized into permanent legislation. This pattern mirrors the challenges faced by medical personnel in managing personal data within digital health systems: technological innovation advances rapidly, while the legal protection framework—including specific consent mechanisms for medical personnel—has not yet been comprehensively established.

In the provision of digital healthcare services, many hospital and digital platform policies rely on broad consent clauses contained in employment agreements or terms of use, without distinguishing between consent given for employment-related purposes and consent for processing personal data beyond that relationship. Physicians and nurses are frequently "deemed to have consented" to all forms of data processing carried out within an institution, even though the PDP Law normatively requires clear delineation of purposes and separation of data uses. This practice blurs the boundary between managerial authority and the personal autonomy of medical personnel as data subjects.

From a rights-protection perspective, the inadequate regulation and implementation of the consent principle risk diminishing the professional dignity of medical personnel. When their data is treated merely as an administrative component within digital healthcare systems, without meaningful avenues to express consent for secondary processing, they are effectively positioned as "objects of policy" rather than full legal subjects. Recognizing

the right to privacy and control over personal data is integral to respecting the professional autonomy of physicians and nurses.

Accordingly, in addressing the first research question, it may be concluded that the consent principle under the PDP Law provides a strong normative basis for protecting the personal data of medical personnel. However, when translated into sectoral regulations—particularly Minister of Health Regulation No. 24 of 2022 on Medical Records and the broader digital health innovation framework—the consent principle has not been fully operationalized as a mechanism of control available to doctors and nurses. The state and healthcare institutions rely primarily on authority and public interest, while the individual consent of medical personnel has not been systematically incorporated into the regulatory architecture or the design of digital healthcare systems.

3.2. Legal and Practical Implications and Consequences of Implementing—or Failing to Implement—the Principle of Consent

Legally, disregarding or weakly enforcing the consent principle in the processing of medical personnel's personal data may result in administrative, civil, and even criminal liability under the PDP Law. Data controllers—whether the Ministry of Health, healthcare facilities, or digital health platform operators—may be held responsible if they process, disclose, or disseminate the personal data of medical personnel without a valid legal basis or for purposes exceeding the original scope of collection. For physicians and nurses as data subjects, such violations translate into a loss of control over their personal and professional information, exposure to stigmatization and harassment, and potential threats to their physical and psychological well-being.

In the context of digital health innovation, the integration of electronic medical records, the deployment of national platforms such as SatuSehat, and the expansion of telemedicine have substantially increased the volume and range of data processing involving medical personnel. In the absence of a clear consent framework and strict purpose limitations, data initially gathered for administrative or internal credentialing purposes may readily "migrate" into secondary processing, such as performance analytics, reputation assessments, or even public disclosure. In practice, this can generate insecurity among medical personnel and contribute to resistance toward digital health transformation policies.

Loss of control over personal data affects not only legal protections but also the professional dignity of doctors and nurses. When data such as disciplinary histories, performance evaluations, or personal information is accessed or distributed without proper consent, professional reputations may suffer damage even before ethical or legal processes are concluded. In some cases, medical personnel may face forms of "social punishment" that far exceed formal institutional sanctions. This undermines the principles of procedural fairness and the presumption of innocence fundamental to a state governed by the rule of law.

The alleged sexual harassment case involving an obstetrician identified by the initials MSF in Garut illustrates how the personal data of medical personnel can be widely exposed in the public sphere. Criminally, the individual may be held accountable under the TPKS Law and the professional code of ethics. Nonetheless, the extensive reporting, circulation of CCTV footage, and disclosure of the individual's professional identity and profile across various media and social platforms demonstrate how the boundary between public interest and the perpetrator's right to privacy as a data subject becomes blurred. In the absence of a clear personal data protection framework, such exposure can shift easily from serving evidentiary or preventive purposes to a form of "trial by media," disregarding the principle of proportionality.

Similarly, the sexual assault case involving a PAP resident doctor at RSHS Bandung illustrates the complex relationship between malpractice, sexual violence, and hospital governance. Reports suggest that weaknesses in managerial oversight, including inadequate control over anesthetic access and insufficient supervision of operating rooms, enabled the recurrence of such violence. From a data protection standpoint, the case concerns not only a criminal act that must be prosecuted but also the public exposure of the perpetrator's identity, educational background, residency status, and professional record. In the absence of clear guidelines, the boundary between legitimate law-enforcement needs and the public's desire to impose social "punishment" becomes increasingly unclear.

The risks are amplified when the profiles of medical personnel—both perpetrators and uninvolved individuals—are technically linked and integrated into a national digital platform. Data originally collected for administrative and credentialing purposes (such as STR numbers, practice locations, and training histories) may be leaked or accessed by unauthorized parties, then combined with social media content and news coverage. Without privacy-by-design safeguards, purpose limitation, and clear consent for secondary processing, physicians and nurses may face multiple harms: beyond criminal or disciplinary proceedings, they may lose control over their personal and professional data outside legitimate law-enforcement contexts. At the same time, it must be acknowledged that, in cases of sexual violence or other serious misconduct, there is a legitimate public interest in disclosing the perpetrator's identity to protect potential victims, prevent recurrence, and ensure accountability within healthcare institutions. The normative challenge lies in balancing this public interest with the consent and purpose-limitation principles under the PDP Law. Without clear procedural guidance and effective control mechanisms, there is a risk that law-enforcement agencies, media, and the public may assume that all data "related to the perpetrator" can be disseminated without restriction, even though the PDP Law requires that data processing remain proportional, relevant, non-excessive, and confined to lawful purposes.

Research on telemedicine further supports these concerns. Findings show that weak legal protection for doctors and patients in remote healthcare services—stemming from limited regulatory instruments, insufficient institutional structures, and an underdeveloped

legal culture—has undermined the fairness and effectiveness of service delivery. A similar pattern appears in digital health innovations that manage electronic medical records and medical personnel profiles: when physicians and nurses perceive their personal data as easily exploited without explicit consent, they tend to adopt defensive attitudes and become reluctant to participate fully in reporting systems, research activities, or innovations requiring data sharing. In practice, this can diminish data quality, impede systemic learning from cases of sexual violence and malpractice, and ultimately hinder broader efforts to improve the quality of healthcare services.

From a legal standpoint, disregarding the consent principle opens the possibility for various forms of disputes. First, administrative disputes may arise between medical personnel and regulators, such as objections to the inclusion or publication of profiles in national systems without sufficient consent. Second, civil disputes may take the form of claims for damages stemming from reputational harm, loss of employment opportunities, or threats to personal safety resulting from data leaks or misuse. Third, ethical or disciplinary disputes may occur when professional organizations find that data management practices within healthcare institutions violate medical or nursing codes of ethics. The lack of a clear operational framework for consent leaves each of these potential disputes in a legal gray area.

In practical terms, applying the consent principle to the personal data of medical personnel should not be interpreted as an impediment to the public interest or to digital health innovation. When implemented through a "consent-plus" approach—combining consent with privacy-by-design features, role-based access control, access logging, and de-identification mechanisms—the state can still manage medical data for epidemiological research, policy development, and service quality evaluation without compromising the dignity or reputation of medical personnel. The public, for example, can be informed when a doctor receives administrative sanctions or has a license revoked without the need to disclose personal data irrelevant to public protection.

In digital healthcare practice, several concrete measures may be taken: clarifying consent clauses in employment agreements and privacy policies; distinguishing between consent for legally mandated data processing and optional secondary uses; providing a dashboard or channel enabling medical personnel to review, correct, and object to the processing of their personal data; and involving professional organizations in developing data protection standards specific to medical personnel. Through such measures, the consent principle becomes not merely a normative provision in the PDP Law but an institutional practice embedded within digital healthcare systems.

In addressing the second research question, it can be concluded that the weak or neglected application of the consent principle in the protection of medical personnel's personal data carries serious legal and practical consequences: potential violations of the PDP Law, reputational and psychological harm to doctors and nurses, reduced trust in digital healthcare systems, and heightened risk of public persecution. Cases involving

sexual violence followed by excessive exposure of medical personnel's identities clearly illustrate the dangers posed by an absence of a robust consent framework and adequate data protection design. Therefore, any digital health innovation involving the personal data of medical personnel must be grounded in, and constrained by, the consent principle as mandated by the PDP Law, ensuring that the public interest, victims' rights, and the professional dignity of doctors and nurses are equally safeguarded.

4. CONCLUSION

A normative analysis of the PDP Law and Minister of Health Regulation No. 24 of 2022 shows that the consent principle has been formally recognized as the lawful basis for processing the personal data of medical personnel, particularly physicians and nurses. Yet its implementation within the digital health ecosystem remains weak and inconsistent, offering limited control for medical personnel as data subjects. Sectoral regulations that emphasize medical record integration and state authority, without clear consent mechanisms, have produced legal and practical risks, including potential violations of the PDP Law, reputational harm, uncertainty over privacy rights, and declining trust in digital health systems. Recent cases involving sexual violence accompanied by excessive disclosure of perpetrators' identities demonstrate that, without a robust consent framework and adequate data protection design, medical personnel may face disproportionate exposure and significant harm.

Reform is therefore essential. The government must align sectoral regulations with the PDP Law by embedding explicit consent mechanisms, privacy-by-design principles, access limits, audit trails, and redress procedures into Ministerial Regulation No. 24/2022 and SatuSehat policies. Regulators and the judiciary should also develop technical and jurisprudential guidelines that establish consent as a standard for personal data processing in healthcare. Healthcare facilities need internal policies and SOPs that classify personnel data, restrict processing purposes, require written consent for secondary uses, provide regular PDP training, and strengthen information system security through role-based access and encryption.

Medical personnel, in turn, must enhance legal and digital literacy, critically review consent clauses in employment and platform agreements, and actively exercise their rights to information, correction, and objection. Professional organizations such as IDI and PPNI should incorporate personal data protection into ethical codes and practice standards. Through these measures, the consent principle can move beyond an abstract legal requirement and function as a practical safeguard that supports trust in digital health services.

REFERENCES

Journals

Anwary, Ichsan, dan Rusma Wahyudi. "Perlindungan Hukum Terhadap Dokter, Dokter Gigi dan Pasien Pada Penerapan Rekam Medis Elektronik di Rumah Sakit." *Badamai Law Journal* 6, no. 1 (2021): 150–69. https://doi.org/10.32801/damai.v6i1.11755.

Caturjayanti, Vermonita Dwi. "Konsep Privacy by Design sebagai Perlindungan Data Pribadi Pengguna Aplikasi 'Peduli Lindungi.'" *Rewang Rancang: Jurnal Hukum Lex Generalis* 1, no. 9 (2020): 70–87. https://doi.org/10.56370/jhlg.v1i9.251.

Dewi, Gusti Ayu Made Purnama, dan I Putu Gede Adiatmika. "Legal and Ethical Analysis of the Implementation of Informed Consent in Medical Practice in Indonesia." *Babali Nursing Research* 6, no. 3 (2025): 578–85. https://doi.org/10.37363/bnr.2025.63491.

Fauzy, Elfian, dan Nabila Alif Radika Shandy. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissance* 7, no. 3 (2023): 445–61. https://doi.org/10.20885/JLR.vol7.iss3.art1.

Kikhau, Erlen Enjelita, Rudepel Petrus Leo, dan Debi F.Ng Fallo. "Pelaksanaan Persetujuan Tindakan Medis (Informed Consent) Sebagai Upaya Perlindungan Hukum Bagi Tenaga Medis dan Pasien." *Jurnal Hukum Bisnis* 12, no. 6 (2023): 1–10. https://doi.org/10.47709/jhb.v12i06.3073.

Kurniawan, Alfian Listya, dan Anang Setiawan. "Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19." *Jurnal Hukum dan Pembangunan Ekonomi* 9, no. 1 (2021): 95–112. https://doi.org/10.20961/hpe.v9i1.52586.

Masidin. "Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Jurnal Hukum: Officium Nobile* 1, no. 1 (2024): 1–12. https://journal.unas.ac.id/jhon/article/view/3866.

Ramadhani, Cahyadi, Nayla Alwiya, dan Ulil Afwa. "Perlindungan Hukum Perekam Medis Dalam Pelayanan Rekam Medis dan Informasi Kesehatan di Fasilitas Pelayanan Kesehatan." *Soedirman Law Review* 3, no. 2 (2021): 1–12. https://doi.org/10.20884/1.slr.2021.3.2.149.

Riasari, R. H. "Perlindungan Hukum terhadap Perawat pada Rumah Sakit Berdasarkan Undang-Undang Nomor 38 Tahun 2014 tentang Keperawatan." *Rewang Rancang: Jurnal Hukum Lex Generalis* 2, no. 10 (2021): 946–60. https://doi.org/10.56370/jhlg.v2i10.79.

Siregar, Rospita Adelina, dan Nanin Koeswidi Astuti. "Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia." *International Journal of Law, Policy and Social Review* 7, no. 3 (2025): 15–21. https://www.lawjournals.net/archives/2025/7/3/7062.

Widjaja, Gunawan, Wagiman, Dyah Ersita Yustanti, Hotmaria Hertawaty Sijabat, dan

Handojo Dhanudibroto. "Perlindungan Hukum Bagi Pasien dan Tenaga Medis Dalam Inovasi Kesehatan Digital: Tinjauan Literatur Terhadap Peraturan Perundang-Undangan di Indonesia." *JK: Jurnal Kesehatan* 3, no. 2 (2025): 200–210. https://wikep.net/index.php/JUKESAH/article/view/268/242.

Winarti, dan Rizka. "Informed Consent sebagai Upaya Perlindungan Hukum Bagi Tenaga Kesehatan dalam Kasus Medis Darurat (Studi Kasus di Rumah Sakit Umum Daerah Provinsi Papua Barat)." *Sehat Rakyat Jurnal Kesehatan Masyarakat* 4, no. 2 (2025): 264–77. https://doi.org/10.54259/sehatrakyat.v4i2.4310.

Proceeding

Wardana, I Wayan Dody Putra, I Gede Diki Sudarsana, Putu Ayu Sri Murcittowati, dan Made Karma Maha Wirajaya. "Legal Protection for Medical Recorders and Health Information Personnel in the Management of Electronic Medical Records." In *Procedia of Engineering and Life Science Universitas Muhammadiyah Sidoarjo*. Sidoarjo: Universitas Muhammadiyah Sidoarjo, 2025. https://doi.org/10.21070/pels.v7i0.2091.

Books

Sadi, Muhamamad Is. *Etika dan Hukum Kesehatan*. Jakarta: Kencana, 2010.

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: UII Press, 2012.

Sugiyono. *Metode Penelitian Kualitatif*. Bandung: Rake Sarasin, 2020.

Yew, Gary Chan Kok, dan Michael Yip. *Data and Private Law: Translating Theory into Practice*. Oxford: Hart Publishing, 2021.

Website

Tempo. "Kronologi Pemerkosaan 2 Korban Baru Dokter Priguna." Tempo.co.id, 2025. https://www.tempo.co/hukum/kronologi-pemerkosaan-2-korban-baru-dokter-priguna-1230771.

Regulations

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran.

Undang-Undang Nomor 38 Tahun 2014 tentang Keperawatan.

Permenkes No. 24 Tahun 2022 tentang Rekam Medis.