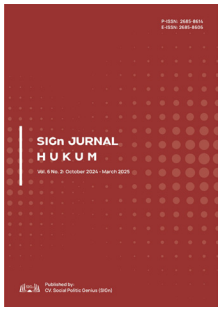

SIGn Jurnal Hukum

E-ISSN: 2685 – 8606 || P-ISSN: 2685 – 8614
https://jurnal.penerbitsign.com/index.php/sjh/article/view/v7n1-24

Vol. 7 No. 1: April - September 2025 Published Online: August 27, 2025

Article Title

Ethics and Law of Personal Data Protection for Smartwatches in the Healthcare Sector

Author(s)

Hartono Tasir Irwanto*
Universitas Hasanuddin, Indonesia || hartonotasir@unhas.ac.id
**Corresponding Author*

Wiranti Wiranti
Universitas Hasanuddin, Indonesia || wiranti@unhas.ac.id

Muhammad Fitratallah Dahlan
Universitas Hasanuddin, Indonesia || muh.fitratallahdahlan@unhas.ac.id

Nadiah Khaeriah Kadir
Universitas Hasanuddin, Indonesia || nadiahkhaeriah@unhas.ac.id

How to cite:

Irwanto, H. T., Wiranti, W., Dahlan, M. F., & Kadir, N. K. (2025). Ethics and Law of Personal Data Protection for Smartwatches in the Healthcare Sector. *SIGn Jurnal Hukum, 7*(1), 421-436. https://doi.org/10.37276/sjh.v7i1.489

ABSTRACT

The rapid adoption of smartwatches in the healthcare sector presents a fundamental duality between the potential for medical innovation and systemic risks to the right to privacy. This research aims to critically analyze the juridical-ethical gap between the health data governance practices of the smartwatch industry and the normative standards mandated by Law Number 27 of 2022. Using a normative legal research method and a gap analysis approach, this study dissects how industry practices systematically create a transparency deficit and devalue the meaning of informed consent into an illusory agreement. The analysis reveals a diametrical opposition between the regulatory ideal (das sollen), which prioritizes user autonomy, and the reality of industry practices (das sein), which are driven by commercial interests and formalistic compliance. This gap not only exposes users to data exploitation but also challenges the effectiveness of Law Number 27 of 2022 in addressing the complexity of wearable technology. Therefore, this research recommends a paradigm shift from the fragile consent-based model to a rights-based model. Furthermore, it urges the formulation of specific implementing regulations for the health technology sector to bridge the existing gap and build a fair and accountable digital ecosystem.

Keywords: *Health Law; Informed Consent; Personal Data Protection; Smartwatch; Wearable Technology.*

INTRODUCTION

The digital revolution has fundamentally transformed the healthcare sector, ushering in a new era of personalized, proactive, and data-driven medical services (Karrouk et al., 2025). At the epicenter of this transformation, wearable technology, particularly smartwatches, has emerged as a significant instrument in the democratization of personal health monitoring. These devices offer advanced capabilities, from tracking heart rates and oxygen saturation to monitoring sleep patterns, enabling individuals to participate in their own health management actively. The benefits extend beyond enhancing individual awareness, holding substantial potential to support early diagnosis, chronic disease management, and the overall efficiency of the healthcare system.

However, beneath these functional advantages lies a complex ethical and legal dilemma. The health data continuously collected by smartwatches constitutes the most sensitive and personal information. Consequently, its collection, storage, and utilization present formidable challenges to the fundamental right to privacy. Each record of a heart rate or sleep cycle is a digital footprint of an individual's biological condition, which, if not managed with the principle of due care, is susceptible to misuse. The balance between technological innovation that drives medical advancement and the protection of personal data as a pillar of human dignity has now become a critical discourse in the legal and ethical arenas (Soemitro et al., 2023).

In response to this challenge, jurisdictions worldwide have developed regulatory frameworks for data protection. The GDPR in the European Union has

become a global gold standard, while Indonesia has enacted Law Number 27 of 2022. Nevertheless, these regulations are typically designed as a general framework and may not be adequate to address the unique characteristics of the wearable technology ecosystem. The passive and continuous nature of data collection, coupled with a data processing chain involving various actors—from device manufacturers and application developers to cloud computing service providers—creates a complexity that surpasses conventional data processing scenarios.

This regulatory gap is exacerbated by the absence of specific technical rules that explicitly govern health data from wearable devices. As a result, a legal grey area has emerged, creating uncertainty for consumers, the industry, and law enforcement. Fundamental principles such as justice and legal certainty, along with essential ethical demands for transparency in data processing and the validity of informed consent, are often not comprehensively accommodated (Mone & Shakhlo, 2023). This chasm between ideal ethical norms and the practical implementation of legal principles necessitates a holistic approach to ensure user privacy is protected without sacrificing the potential for technological innovation.

Previous academic literature has identified several dimensions of this issue. For instance, a cross-sectional survey by Cilliers (2020) highlighted that a majority of smartwatch users possess a low level of understanding regarding the importance and mechanics of their health data protection. Similarly, research by Jiang and Shi (2021) underscored the privacy paradox, a phenomenon where users tend to disregard significant privacy risks in exchange for the convenience and practical benefits offered by these devices. Both studies validly demonstrate a problem at the level of user awareness.

However, focusing solutions solely on user education, as implied by previous research, is an inadequate approach. Such an argument inherently places a disproportionate burden of data protection on the individual, while ignoring systemic issues, namely opaque industry practices and the absence of significant consent mechanisms. Education becomes ineffective when users are confronted with lengthy, ambiguous privacy policies presented on a take-it-or-leave-it basis. Therefore, the actual research gap lies not only in the lack of user understanding but also in the critical analysis of the failure of legal frameworks and system designs to uphold the principle of user autonomy.

It is here that the principle of informed consent assumes a central role, not merely as a legal formality but as an ethical manifestation of respect for individual autonomy. Genuine informed consent requires a user's complete comprehension of how, for what purpose, and by whom their data will be processed (Cheng et al., 2024). In the current smartwatch ecosystem, consent mechanisms are often reduced to the

act of clicking a checkbox—an illusion of choice that fails to reflect conscious and voluntary agreement. This research argues that the emphasis must shift from merely educating users to mandating that the industry design systems that are transparent and empower users to provide authentic consent.

The Indonesian context presents a particularly relevant and urgent case study. As a nation with a massive digital penetration rate and rapid growth in wearable technology adoption, Indonesia represents a crucial testing ground for the implementation of Law Number 27 of 2022. The combination of swift technological adoption, a developing societal level of data privacy literacy, and a field-untested legal framework creates an environment vulnerable to the risks of data exploitation. Analyzing this issue within the Indonesian context is not only domestically relevant but also offers insights for other developing countries facing similar digitalization trajectories.

Based on this background, this research has a focused objective. Broadly, it aims to critically analyze the alignment of data management practices for smartwatch-generated health data with ethical standards and the legal framework for personal data protection in Indonesia. Specifically, its objectives are: (1) to identify and analyze the implementation gaps of privacy principles, informed consent, and transparency within the smartwatch ecosystem; (2) to evaluate the effectiveness and challenges of applying Law Number 27 of 2022 to regulate wearable health technology; and (3) to formulate juridical-ethical recommendations for creating a more equitable and accountable data governance model. The benefits of this research are twofold. Theoretically, it contributes to the literature on health and technology law by offering the first in-depth analysis of the implementation of Law Number 27 of 2022 concerning wearable devices. Practically, this research is expected to produce concrete guidance for regulators in drafting implementing regulations and for industry stakeholders in designing more ethical and legally compliant products and policies.

METHOD

This study is structured as normative legal research, focusing on the analysis of legal norms, principles, and doctrines in relation to the issue of personal data protection. This approach was selected because the central problem addressed involves normative voids and conflicts between the rapidly evolving practices of smartwatch technology and the prevailing legal and ethical frameworks. The nature of this research is prescriptive-analytical; that is, it aims not only to describe existing legal phenomena but also to conduct a critical evaluation and formulate concrete recommendations (Qamar & Rezah, 2020). Accordingly, this study will systematically identify, analyze, and ultimately present an argument on how the law ought to respond to the ethical challenges posed by wearable health technology.

The data sources for this research are derived entirely from library materials collected through a literature study technique (Sampara & Husen, 2016). These sources are classified into three categories. *First*, primary legal materials, which include binding statutory regulations, particularly Law Number 27 of 2022, and the constitutional foundation within the 1945 Constitution. *Second*, secondary legal materials, which consist of sources that provide analytical explanations of primary legal materials, such as reputable academic journals, books, and relevant prior research. The selection of secondary materials was prioritized based on criteria of currency, topical relevance, and the academic authority of the authors. *Third*, tertiary legal materials, such as legal dictionaries and encyclopedias, were used to provide conceptual and terminological clarification.

All collected data were analyzed qualitatively using a critical-comparative approach. This analytical process comprised several systematic stages (Irwansyah, 2020). The first stage was juridical interpretation, wherein relevant articles in Law Number 27 of 2022 and associated regulations were interpreted to establish normative benchmarks for the principles of privacy, informed consent, and transparency. The second stage was practice identification, which involved identifying smartwatch industry practices in health data management as documented in secondary legal materials. The third stage, the core of this research, was a gap analysis. Here, the identified industry practices were critically compared and evaluated against the established normative benchmarks. This analysis was directly aimed at addressing the research objectives by dissecting the points of divergence between the reality (*das sein*) and the ideal legal and ethical norms (*das sollen*). Based on the results of this gap analysis, the final stage was synthesis and the formulation of recommendations, wherein prescriptive solutions were logically and justifiably constructed to bridge the existing gaps.

RESULTS AND DISCUSSION

A. The Duality of Health Data Governance: Between Regulatory Ideals and Industry Realities

A thorough analysis of health data governance for smartwatch-generated data reveals a fundamental duality: a diametrical opposition between ideal normative standards (*das sollen*) and prevailing industry practices (*das sein*). On one hand, contemporary legal and ethical frameworks strive to construct a robust protective framework founded on the pillars of individual autonomy, human dignity, and the fundamental right to privacy. On the other hand, the reality, driven by commercial dynamics and technical complexities, fosters practices that systematically erode these protective foundations. To comprehensively dissect the root of the problem,

the crucial first step is to clearly map these two opposing poles: the normative benchmarks that constitute the ideal and the industry practices that represent the problematic reality.

1. Mapping Normative Benchmarks: Philosophical, Constitutional, and Legislative Foundations

The normative benchmark for health data protection does not exist in a vacuum. It is deeply rooted in well-established philosophical-ethical grounds that recognize the right to privacy as an essential manifestation of individual autonomy and dignity. In this view, every individual is a sovereign legal subject with authority over information concerning themselves, particularly health data, which reflects the most intimate and vulnerable conditions of their biological existence (Compagnucci et al., 2022). Respect for this autonomy transcends mere moral obligation; it is a fundamental prerequisite for building and maintaining trust within the health technology ecosystem. Without solid trust, the transformative potential of technology to improve the quality of life will forever be hindered by public apprehension regarding the risks of surveillance, manipulation, and data misuse. This, in turn, can damage individual integrity and delegitimize the innovation itself (Jiang & Shi, 2021).

This constitutional guarantee is further translated into a more operational and comprehensive legislative framework through Law Number 27 of 2022. The enactment of this Law marks a new era in data governance in Indonesia, shifting from a fragmented and partial regulatory approach to an integrated legal regime. Significantly, Law Number 27 of 2022 classifies health data and information as "specific Personal Data." This classification is not merely terminological; it carries severe legal consequences. Health data de jure demands a higher level of protection, stricter processing requirements, and a more limited legal basis for processing compared to general personal data.

Based on a systematic and teleological interpretation of Law Number 27 of 2022, and with reference to the universal principles recognized in the GDPR, the normative benchmarks for smartwatch data controllers can be detailed as three primary, non-negotiable obligations. First is the obligation of absolute transparency, which requires the provision of clear, concise, easily accessible information, written in plain language, regarding all aspects of data processing. Second is the acquisition of valid and meaningful informed consent, which necessitates that consent be explicit, conscious, voluntary, and specific for each processing purpose, and it must be as easy to withdraw as it is to give. Third is the implementation of the principles of data minimization and

purpose limitation. This principle obligates data controllers to collect only data that is relevant and strictly necessary for the consented purpose and strictly prohibits the processing of such data for other, incompatible purposes without obtaining new consent. These three pillars collectively form the ideal standard (*das sollen*) that must be adhered to by every entity within the smartwatch ecosystem.

Based on a systematic and teleological interpretation of Law Number 27 of 2022, and with reference to the universal principles recognized in the GDPR, the normative benchmarks for smartwatch data controllers can be detailed as three primary, non-negotiable obligations. *First* is the obligation of absolute transparency, which requires the provision of clear, concise, easily accessible information, written in plain language, regarding all aspects of data processing. *Second* is the acquisition of valid and meaningful informed consent, which necessitates that consent be explicit, conscious, voluntary, and specific for each processing purpose, and it must be as easy to withdraw as it is to give. *Third* is the implementation of the principles of data minimization and purpose limitation. This principle obligates data controllers to collect only data that is relevant and strictly necessary for the consented purpose and strictly prohibits the processing of such data for other, incompatible purposes without obtaining new consent. These three pillars collectively form the ideal standard (*das sollen*) that must be adhered to by every entity within the smartwatch ecosystem.

2. Identifying Industry Practices: The Realities of Security, Formalistic Compliance, and Data Commercialization

However, an examination of industry practices (*das sein*) as documented in various academic literatures presents a starkly contrasting picture to the normative ideal. The reality on the ground is shaped by three primary forces: technical complexity, the demand for formalistic compliance, and powerful incentives for data commercialization. The modern smartwatch ecosystem involves a highly complex and fragmented data processing chain, often engaging dozens, if not hundreds, of different entities. These range from device manufacturers, application developers, and cloud computing providers to data brokers and third-party researchers (Elngar et al., 2021; Ioannidou & Sklavos, 2021). This fragmentation creates extraordinary challenges in ensuring clear accountability and applying consistent data security standards across the entire value chain.

Consequently, rigorous cybersecurity approaches, which are theoretically an absolute necessity for sensitive health data, often conflict

with technical limitations such as the processing power and connectivity of wearable devices. Furthermore, business models inherently designed to prioritize the massive and continuous collection and transmission of data also pose a constraint (Fornasier, 2019). Vulnerabilities to cyberattacks and data breaches are not theoretical risks; they are persistent, tangible threats lurking within the current system architecture.

From a regulatory compliance perspective, many multinational health technology companies operating in Indonesia strive to demonstrate adherence to leading international standards, such as the GDPR in the European Union or regulations from the FDA in the United States (Brönneke et al., 2021; Hassanaly & Dufour, 2021). However, a deeper analysis reveals that this compliance is often formalistic and procedural rather than substantive. For instance, the privacy policies presented to users are typically lengthy legal documents, written in ambiguous legal jargon and designed more as a legal shield to protect the company from potential future litigation than as an instrument to empower users to make an informed consent.

This practice effectively creates "consent fatigue" among users, who become accustomed to agreeing to terms and conditions without reading them. As a result, the consent mechanism, which should be the culmination of the exercise of individual autonomy, is reduced to a mere mechanical act of clicking a checkbox—a ritual devoid of adequate understanding. It can be termed the reality of formalistic compliance: satisfying the letter of the law on paper while disregarding its spirit and ultimate purpose.

Furthermore, and most consequentially, is the massive drive for data commercialization. Aggregated and individual health data possess extremely high economic value in the market, becoming a valuable commodity for the insurance, pharmaceutical, and advertising industries, as well as various other actors. This financial incentive creates immense pressure on companies to formulate vague and overly broad consent clauses. These clauses enable them to use, share, or sell data for secondary purposes that were never specifically realized or agreed to by the user. Such practices risk transforming the user from a sovereign legal subject over their data into an object of data exploitation—a phenomenon that ethical critics have termed a form of predatory marketing that endangers users in the name of innovation (Predel & Steger, 2021).

3. Affirming the Fundamental Duality as the Point of Analysis

The stark comparison between the normative benchmarks (*das sollen*) and the reality of industry practices (*das sein*) decisively confirms the existence

of a fundamental duality that lies at the core of the problem. On one side, law and ethics mandate a user-centric system wherein transparency, autonomy, and individual control are inviolable principles. This system regards the user as a rights-holder who must be protected.

On the other side, industry practices—driven by technical complexity, formalistic compliance, and powerful commercial incentives—have created a de facto business-centric system. In this system, transparency is often replaced by intentional opacity, consent becomes illusory, and users effectively lose meaningful control over their most personal health data. This duality is the primary source of the juridical-ethical tension in the use of smartwatches in the healthcare sector. It is not merely a minor discrepancy; it is a deep chasm between the promise of legal protection and the reality of user vulnerability. This chasm will serve as the point of departure and the central focus of the gap analysis to be dissected in depth in the following section.

B. Juridical-Ethical Gap Analysis and Its Implications for User Protection

Proceeding from the fundamental duality previously mapped, the next stage of analysis is to systematically dissect the points of divergence between regulatory ideals and industry realities. This gap analysis constitutes the core of the research, aiming to precisely identify how and why current smartwatch data governance practices fail to meet the normative standards mandated by law and ethics. This gap is not monolithic; it manifests in several critical, interconnected dimensions, ranging from a transparency deficit and the devaluation of informed consent to challenges to regulatory effectiveness itself. Each of these dimensions will be analyzed in depth to understand the root causes and their implications for user protection.

1. The Transparency Deficit and the Creation of Information Asymmetry

The first and most fundamental gap lies in the transparency deficit. The transparency obligation under Law Number 27 of 2022 requires that information regarding data processing be presented clearly, concisely, and understandably. The objective is to empower the data subject to make autonomous decisions. However, industry practices systematically create the opposite condition: information asymmetry, wherein the company, as the data controller, possesses vastly superior knowledge regarding data flows and utilization compared to the user. This asymmetry is intentionally created and maintained through the instrument of opaque privacy policies.

Privacy policy and terms of service documents are generally not designed to inform; instead, they are crafted to secure the company's legal

position (Smart & McManus, 2022). The use of complex legal jargon, convoluted sentences, and ambiguous clauses makes these documents nearly impossible for a layperson to comprehend. Crucial information—such as the third parties who will receive the data, the purposes of data processing for internal company interests like algorithm development, or data retention periods—is often concealed within thousands of words. This practice directly contravenes the principle of transparency, as information that cannot be understood is effectively tantamount to a complete lack of information.

This transparency deficit is compounded by the inherent technical vulnerabilities of the Internet of Things (IoT) ecosystem, which includes smartwatches (Fornasier, 2019). Limitations in bandwidth and processing power are often cited as reasons for not implementing strong encryption or layered security mechanisms, which create openings for unauthorized access by third parties (Elngar et al., 2021). Information regarding these technical security levels is rarely disclosed transparently to users. Consequently, users are not only in an informationally disadvantaged position regarding company policies but are also vulnerable to the tangible cybersecurity risks that threaten their most sensitive health data (Batista et al., 2021).

2. The Devaluation of Informed Consent into Illusory Agreement

The second gap, which is most detrimental to user autonomy, is the devaluation of the concept of informed consent. Juridically and ethically, informed consent is a dialogical process that requires three cumulative elements: adequate information (the "informed" component), voluntariness, and the subject's competence to grant consent. The practices of the smartwatch industry have reduced this sacrosanct process to a single, superficial act: clicking a consent box or an "I Agree" button.

This practice, known as clickwrap consent, is fundamentally legally flawed when measured against the standards of Law Number 27 of 2022. First, the "informed" element is not met, as the information is presented in a non-transparent format, as previously analyzed. Second, the "voluntary" element becomes highly problematic. In a "take-it-or-leave-it" model, the user possesses no bargaining power. The choice presented is not between consenting or not consenting to data processing; the actual choice is between using the device with all its privacy consequences or not using the device at all. It is not a free choice; it is a form of coerced compliance.

Furthermore, the technology industry frequently employs "dark patterns" in user interface (UI) and user experience (UX) design to manipulate users

into giving consent (Nelissen & Funk, 2022). The "Agree" button is made more visually prominent, while options to decline or manage privacy preferences are concealed within multi-layered menus. These manipulative practices blatantly violate the voluntary spirit of informed consent. Consequently, the consent obtained is not an authentic expression of the user's will but rather an illusory agreement engineered by the system's design.

The "privacy paradox"—where users express concern for privacy but in practice still surrender their data—is often used as a justification by the industry. However, this argument is flawed because it ignores the context of user powerlessness. Users do not surrender their data because they do not care; they do so because they feel they have no absolute control and are trapped in an unbalanced privacy calculus (Princi & Krämer, 2020). Thus, consent given under conditions of information asymmetry and limited choice cannot be considered legally valid.

3. Challenges to the Effectiveness of Law Number 27 of 2022 in Addressing Technological Complexity

The third gap lies in the challenge to the effectiveness of Law Number 27 of 2022 itself. As an umbrella law, Law Number 27 of 2022 establishes crucial general principles. However, its technology-neutral character makes it difficult to address the unique characteristics and technical complexities of the smartwatch ecosystem without more specific implementing regulations.

One of the primary challenges is regulating passive, continuous, and contextual data collection. Unlike filling out a data form, which is an active measure, a smartwatch collects biometric data continuously in the background. How can a meaningful informed consent mechanism be applied in this context? Is a single consent at the initial application setup sufficient to legitimize years of data collection? Law Number 27 of 2022 does not yet provide technical answers to these questions.

Another challenge is law enforcement within a fragmented and transnational data ecosystem. Data collected by a smartwatch in Indonesia may be stored on servers in another country and processed by dozens of affiliated companies spread across the globe. Accountability and jurisdictional mechanisms become exceedingly complicated in this scenario. Without strong international cooperation and clear technical guidelines on cross-border data transfers for health data, the enforcement of data subject rights guaranteed by Law Number 27 of 2022 risks becoming ineffective.

Therefore, the argument that strong regulation will stifle innovation must be inverted. It is precisely the absence of precise technical regulation that creates legal uncertainty, which can harm both consumers and the industry in the long term. Effective regulation is not a barrier; it is a framework that provides certainty and enables responsible and sustainable innovation (Damayanti & Priyono, 2022), one in which fundamental human rights are not sacrificed at the altar of technological progress (Tom et al., 2020).

4. Legal and Ethical Implications of the Existing Gaps

The fourth gap, the identified juridical-ethical chasm, carries profound implications for individual users, the industry, and the digital health ecosystem as a whole. For users, the consequences extend beyond a mere loss of privacy. Leaked or misused health data can lead to tangible harm, such as discrimination by insurance companies or employers, unfair profiling, behavioral manipulation, and social stigma (Papa et al., 2018). In the worst-case scenario, this data could be used for malicious purposes that threaten an individual's physical and mental security.

For the industry, ignoring these gaps is a high-risk strategy. Negligence in obtaining valid informed consent and the failure to provide transparency constitute direct violations of Law Number 27 of 2022. The legal consequences are unequivocal, encompassing severe administrative sanctions, civil damages claims from data subjects, and potential criminal sanctions for the corporation or its directors, as stipulated in the Law. The argument that such practices are the "industry standard" will not serve as a valid defense before the law (Sun et al., 2020).

At the macro level, the most damaging implication is the erosion of public trust. The health technology ecosystem can only thrive if it is based on strong societal trust (Sui et al., 2023). Every incident of a data breach or privacy misuse scandal will significantly damage this trust, ultimately slowing the adoption of beneficial health technologies and hindering the realization of the positive potential of digital innovation (Brönneke et al., 2021). Thus, bridging this juridical-ethical gap is not merely a matter of legal compliance; it is a strategic imperative to ensure a future for health technology that is secure, equitable, and sustainable.

CONCLUSIONS AND SUGGESTIONS

Based on the results and discussion, it is concluded that a significant and systemic juridical-ethical gap exists between the health data governance practices of smartwatches and the legal framework for personal data protection in Indonesia. This gap critically manifests in three primary dimensions. *First*, a transparency deficit that creates a detrimental information asymmetry for users. *Second*, the devaluation of informed consent into an illusory agreement through the practices of clickwrap consent and manipulative design. *Third*, challenges to the effectiveness of Law Number 27 of 2022 as an umbrella law that has not yet been able to address the technical complexities of the wearable ecosystem. These findings decisively answer the research objectives, confirming that current data management by smartwatches is not aligned with the ethical and legal standards that prioritize user autonomy and protection.

The theoretical implication of this research is the strengthening of the technology law discourse, which emphasizes that formalistic compliance with regulations is insufficient to realize substantive data protection. A paradigm shift is required from the demonstrably fragile consent-based model to a rights-based model that positions the rights of the data subject as the primary foundation. Practically, this study provides a strong argumentative basis for regulators, industry stakeholders, and civil society to advocate for data governance reform. Ignoring the existing gaps not only risks severe legal consequences for the industry but also threatens to erode the public trust that is a prerequisite for the sustainable development of the digital health ecosystem.

To bridge these gaps, a series of concrete, multi-stakeholder steps is necessary. For regulators, particularly the Ministry of Communication and Digital Affairs and the forthcoming personal data protection supervisory authority, it is recommended to promptly formulate implementing regulations or technical guidelines specific to the wearable health technology sector. These guidelines should explicitly regulate minimum standards for transparency, for instance, through an easy-to-read privacy dashboard format. Furthermore, they must define granular and contextual informed consent mechanisms for continuous data collection. For industry stakeholders, it is recommended to proactively adopt the principles of privacy by design and by default, meaning the integration of data protection into the entire product development lifecycle, not as a concluding add-on. It includes ethical interface design and provides users with real, easily accessible control over their data. For academics and future researchers, there is an opportunity to conduct empirical studies on the effectiveness of various privacy notification models and consent mechanisms in Indonesia. Additionally, a comparative analysis of regulatory approaches in other countries could provide richer, evidence-based policy input.

REFERENCES

The 1945 Constitution of the Republic of Indonesia. https://www.dpr.go.id/dokumen/jdih/undang-undang-dasar

Batista, E., Moncusi, M. A., López-Aguilar, P., Martínez-Ballesté, A., & Solanas, A. (2021). Sensors for Context-Aware Smart Healthcare: A Security Perspective. *Sensors, 21*(20), 1-60. https://doi.org/10.3390/s21206886

Brönneke, J. B., Müller, J., Mouratis, K., Hagen, J., & Stern, A. D. (2021). Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring. *21*(14), 1-19. https://doi.org/10.3390/s21144937

Cheng, L., Han, J., & Nasirov, J. (2024). Ethical Considerations Related to Personal Data Collection and Reuse: Trust and Transparency in Language and Speech Technologies. *International Journal of Legal Discourse, 9*(2), 217-235. https://doi.org/10.1515/ijld-2024-2010

Cilliers, L. (2020). Wearable Devices in Healthcare: Privacy and Information Security Issues. *Health Information Management Journal, 49*(2-3), 150-156. https://doi.org/10.1177/1833358319851684

Compagnucci, M. C., Wilson, M. L., Fenwick, M., Forgó, N., & Bärnighausen, T. (Eds.). (2022). *AI in eHealth: Human Autonomy, Data Governance and Privacy in Healthcare*. Cambridge University Press. https://doi.org/10.1017/9781108921923

Damayanti, M., & Priyono, E. A. (2022). Legal Consequences for LDMO Disclosing Personal Data of Transacting Parties: A Study of Legal Protection. *SIGn Jurnal Hukum, 4*(2), 221-232. https://doi.org/10.37276/sjh.v4i2.217

Elngar, A., Pawar, A., & Churi, P. (Eds.). (2021). *Data Protection and Privacy in Healthcare: Research and Innovations*. CRC Press. https://doi.org/10.1201/9781003048848

Fornasier, M. D. O. (2019). The Applicability of the Internet of Things (IoT) between Fundamental Rights to Health and to Privacy. *Revista de Investigacoes Constitucionais, 6*(2), 297-321. https://doi.org/10.5380/RINC.V6I2.67592

Hassanaly, P., & Dufour, J. C. (2021). Analysis of the Regulatory, Legal, and Medical Conditions for the Prescription of Mobile Health Applications in the United States, the European Union, and France. *Medical Devices: Evidence and Research, 14*, 389-409. https://doi.org/10.2147/MDER.S328996

Ioannidou, I., & Sklavos, N. (2021). On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. *Cryptography, 5*(4), 1-19. https://doi.org/10.3390/cryptography5040029

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Jiang, D., & Shi, G. (2021). Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare. *Journal of Healthcare Engineering, 2021*(1), 1-7. https://doi.org/10.1155/2021/6656204

Karrouk, Y., Debasa, F., & Sanchez, L. M. F. (2025). The Digital Transformation of Smart Hospitals: Challenges and Opportunities. In M. Ouaissa et al. (Eds.), *Utilizing AI of Medical Things for Healthcare Security and Sustainability* (pp. 1-54). IGI Global Scientific Publishing. http://doi.org/10.4018/979-8-3373-0690-2.ch001

Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1814

Mone, V., & Shakhlo, F. (2023). Health Data on the Go: Navigating Privacy Concerns with Wearable Technologies. *Legal Information Management, 23*(3), 179-188. http://doi.org/10.1017/S1472669623000427

Nelissen, L., & Funk, M. (2022). Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments. *International Journal of Design, 16*(1), 75-92. https://doi.org/10.57698/v16i1.05

Papa, A., Mital, M., Pisano, P., & Giudice, M. D. (2018). E-Health and Wellbeing Monitoring Using Smart Healthcare Devices: An Empirical Investigation. *Technological Forecasting and Social Change, 153*, 1-10. https://doi.org/10.1016/j.techfore.2018.02.018

Predel, C., & Steger, F. (2021). Ethical Challenges with Smartwatch-Based Screening for Atrial Fibrillation: Putting Users at Risk for Marketing Purposes? *Frontiers in Cardiovascular Medicine, 7*, 1-7. https://doi.org/10.3389/fcvm.2020.615927

Princi, E., & Krämer, N. C. (2020). Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IoT Healthcare Devices. *Frontiers in Psychology, 11*, 1-15. https://doi.org/10.3389/fpsyg.2020.582054

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). http://data.europa.eu/eli/reg/2016/679/oj

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Smart, S., & McManus, A. C. (2022). Closing the Gap between UNGPS and Content Regulation/Moderation Practices. *Revista de Direito Internacional, 19*(2), 269-293. https://doi.org/10.5102/rdi.v19i2.8380

Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore. *SIGn Jurnal Hukum, 5*(1), 155-167. https://doi.org/10.37276/sjh.v5i1.272

Sui, A., Sui, W., Liu, S., & Rhodes, R. (2023). Ethical Considerations for the Use of Consumer Wearables in Health Research. *Digital Health, 9*, 1-7. https://doi.org/10.1177/20552076231153740

Sun, N., Esom, K., Dhaliwal, M., & Amon, J. J. (2020). Human Rights and Digital Health Technologies. *Health and Human Rights, 22*(2), 21-32. Retrieved from https://www.hhrjournal.org/2020/12/08/human-rights-and-digital-health-technologies

Tom, E., Keane, P. A., Blazes, M., Pasquale, L. R., Chiang, M. F., Lee, A. Y., & Lee, C. S. (2020). Protecting Data Privacy in the Age of AI-Enabled Ophthalmology. *Translational Vision Science and Technology, 9*(2), 1-7. https://doi.org/10.1167/tvst.9.2.36

United States Code: Title 21 - Food and Drug, Section 393 - Food and Drug Administration. https://www.govinfo.gov/app/details/USCODE-2023-title21/USCODE-2023-title21-chap9-subchapX-sec393