Indonesian Health Justice Review
ISSN: XXXX-XXXXX (Online)
Vol. 3, No. 2, 2026, pp. 139-162
Published online since June 25, 2026

# Unauthorized Recording of Online Medical Consultations: A Patient's Right to Privacy in Telemedicine

**Muhammad Agung***
Universitas Negeri Semarang, Semarang, Indonesia
*agungmuh@gmail.com*

DOI: https://doi.org/10.65815/t7bk0w82

| Submitted: 11-01-2026 | Revised: 19-03-2026, 20-05-2026 | Accepted: 15-06-2026 |
|---|---|---|

*Corresponding Author

## Abstract

Telemedicine consultations frequently involve the transmission and storage of highly sensitive medical information through digital communication systems. The ability to record consultations creates significant risks when recordings are made, stored, or shared without the patient's knowledge or consent. This article examines the legal protection available to patients against unauthorized recording and secondary use of online medical consultations in Indonesia. The research employs a normative juridical method by analyzing patient confidentiality, privacy rights, personal data protection, informed consent, and healthcare provider obligations. The study finds that the legal characterization of consultation recordings may involve overlapping categories of medical information, personal data, and confidential communications, resulting in a complex regulatory environment. Existing rules may provide general protection but do not sufficiently establish specific standards governing the recording, retention, access, and secondary use of telemedicine consultations. This article proposes a consent-centered governance model requiring explicit disclosure of recording practices, defined purposes, limited retention periods, restricted access, and effective mechanisms for patients to exercise control over their information. Such measures are necessary to prevent digital healthcare from weakening established standards of medical confidentiality. Protecting privacy in telemedicine should be regarded not merely as a data protection issue but as an essential component of patient autonomy and health justice.

[*Konsultasi telemedisin seringkali melibatkan transmisi dan penyimpanan informasi medis yang sangat sensitif melalui sistem komunikasi digital. Kemampuan untuk merekam konsultasi menimbulkan risiko signifikan ketika rekaman dibuat, disimpan, atau dibagikan tanpa sepengetahuan atau persetujuan pasien. Artikel ini mengkaji perlindungan hukum yang tersedia bagi pasien terhadap perekaman tanpa izin dan penggunaan sekunder konsultasi medis daring di Indonesia. Penelitian ini menggunakan metode*

*yuridis normatif dengan menganalisis kerahasiaan pasien, hak privasi, perlindungan data pribadi, persetujuan berdasarkan informasi, dan kewajiban penyedia layanan kesehatan. Studi ini menemukan bahwa karakterisasi hukum rekaman konsultasi dapat melibatkan kategori informasi medis, data pribadi, dan komunikasi rahasia yang tumpang tindih, sehingga menghasilkan lingkungan peraturan yang kompleks. Aturan yang ada mungkin memberikan perlindungan umum tetapi tidak cukup menetapkan standar spesifik yang mengatur perekaman, penyimpanan, akses, dan penggunaan sekunder konsultasi telemedisin. Artikel ini mengusulkan model tata kelola yang berpusat pada persetujuan yang mensyaratkan pengungkapan eksplisit praktik perekaman, tujuan yang ditentukan, periode penyimpanan terbatas, akses terbatas, dan mekanisme efektif bagi pasien untuk mengendalikan informasi mereka. Langkah-langkah tersebut diperlukan untuk mencegah layanan kesehatan digital melemahkan standar kerahasiaan medis yang telah ditetapkan. Melindungi privasi dalam telemedisin seharusnya tidak hanya dianggap sebagai masalah perlindungan data, tetapi juga sebagai komponen penting dari otonomi pasien dan keadilan kesehatan.*]

**Keywords:** Telemedicine, privacy, patient confidentiality, medical consultation, informed consent

## Introduction

Telemedicine has developed from a specialized technological arrangement into an increasingly important component of contemporary healthcare delivery. The ability to provide medical advice, diagnosis, follow-up, and selected forms of treatment without requiring physical presence has expanded healthcare access and reduced geographical barriers. At the same time, telemedicine changes the informational environment in which medical care takes place. The conventional consultation occurs within a relatively controlled clinical setting, whereas a virtual consultation may involve communication platforms, cloud infrastructure, electronic medical-record systems, third-party technology providers, and multiple devices. These additional technological layers increase the number of points at which health information can be collected, processed, stored, or accessed. Earlier scholarship already identified confidentiality as a central legal problem in telemedicine, while more recent literature demonstrates that privacy and security remain significant barriers to the responsible adoption of virtual healthcare (Stanberry 1997; Nittari et al. 2020; Houser, Flite, and Foster 2023).

Among the emerging privacy concerns, unauthorized recording deserves particular attention because recording changes the character of the consultation itself. A live medical conversation is ordinarily temporary, even though its clinically relevant contents may subsequently be documented in a medical record. A recording, by contrast, creates a comprehensive audiovisual representation that can

persist independently of the original clinical encounter. It may preserve not only information necessary for diagnosis and treatment but also the patient's facial expressions, voice, emotional responses, domestic environment, family interactions, and incidental statements. The medico-legal literature specifically identifies audiovisual recording of telehealth encounters as raising questions concerning consent, privacy, confidentiality, and medical records (Farmer et al. 2021). The existence of a recording consequently introduces a new informational object whose legal status cannot simply be equated with the patient's initial decision to participate in telemedicine.

The distinction becomes particularly significant because health information is inherently sensitive. Privacy in healthcare is not merely concerned with preventing public dissemination; it also concerns the circumstances under which information is collected and subsequently processed. Solove's influential taxonomy of privacy demonstrates that privacy harms may arise through collection, processing, dissemination, and use rather than only through public exposure (Solove 2006). Similarly, research concerning electronic health records indicates that confidentiality, security, unauthorized access, and inappropriate information practices can undermine patient trust in digital healthcare systems (Shenoy and Appel 2017; Alhuwail et al. 2020). The creation of a recording without the patient's knowledge may therefore represent a privacy problem even if the recording is never leaked publicly. The legal inquiry should begin with whether the provider possessed legitimate authority to create the recording, not merely with whether the recording was subsequently disclosed.

This problem is especially relevant in Indonesia because the legal framework governing health information has undergone substantial development. Law Number 27 of 2022 concerning Personal Data Protection classifies health data and information as specific personal data, thereby recognizing its heightened sensitivity. Law Number 17 of 2023 concerning Health separately recognizes the right to confidentiality of personal health data and information and regulates confidentiality in relation to healthcare and medical records. Minister of Health Regulation Number 24 of 2022 provides a framework for medical records, including electronic medical records, while Government Regulation Number 28 of 2024 establishes implementing provisions under the Health Law. These instruments create an important normative foundation for protecting patients in digital healthcare. Nevertheless, the existence of general privacy and confidentiality provisions does not necessarily answer the more specific question of whether recording an online consultation constitutes an independent processing activity requiring distinct authorization.

The central legal difficulty is therefore the relationship between consent to telemedicine and consent to recording. A patient who accepts an online consultation ordinarily agrees to receive healthcare through a digital medium. That decision should not automatically be understood as agreement to the creation of an audiovisual archive. Informed consent is meaningful only when the individual

understands the material consequences of the decision being made. Literature on telemedicine ethics repeatedly identifies autonomy and informed consent as fundamental principles requiring adaptation to digital healthcare environments (Chaet et al. 2017; Keenan, Tsourtos, and Tieman 2021). Research on electronic informed consent similarly demonstrates that remote consent processes must address understanding, legal validity, privacy, security, and usability rather than treating electronic agreement as a purely formal procedure (De Sutter et al. 2020).

The argument advanced in this article is that recording should be treated as a distinct processing activity because it materially changes the persistence, accessibility, and potential secondary use of information generated during a medical consultation. This proposition does not imply that all recording is unlawful or ethically impermissible. Recording may be justified for legitimate clinical, educational, research, or legal purposes where appropriate legal requirements are satisfied. The problem arises when recording is treated as an automatic consequence of telemedicine participation. International scholarship has emphasized that privacy, confidentiality, consent, and security remain central ethical and legal concerns in telemedicine, while specific literature on audiovisual recordings demonstrates that recording itself creates additional medico-legal questions (Nittari et al. 2020; Farmer et al. 2021).

This article therefore examines how Indonesian law should protect patients against unauthorized recording and subsequent secondary use of telemedicine consultations. It approaches the issue through three interconnected dimensions: the legal characterization of the recording, the relationship between privacy and patient autonomy, and the governance of subsequent processing. The article argues that Indonesian law should move beyond a model that focuses primarily on data security and disclosure toward a lifecycle approach encompassing creation, retention, access, transfer, and reuse. Such an approach is consistent with broader scholarship on telehealth privacy governance, which emphasizes confidentiality, access control, retention, encryption, authentication, and accountability as interconnected components of responsible digital healthcare (Watzlaf et al. 2017; Kuziemsky et al. 2018).

## Theoretical and Conceptual Framework

Privacy in healthcare should be distinguished from confidentiality even though the two concepts are closely related. Privacy concerns the individual's interest in controlling access to personal information and personal space, whereas confidentiality concerns the obligations imposed upon individuals or institutions that legitimately obtain information. Data protection adds a further dimension by regulating the lifecycle of personal information, including its collection, processing, storage, transfer, and deletion. In telemedicine, these dimensions converge because a consultation simultaneously constitutes a confidential professional interaction and a technologically mediated data-processing activity. The literature on

telemedicine consistently identifies privacy and confidentiality as distinct but interrelated challenges, particularly where digital systems involve multiple devices, platforms, and information flows (Norton, Lindborg, and Delaplain 1993; Stanberry 1997; Watzlaf et al. 2017).

The theory of contextual integrity provides a useful framework for understanding why a patient's disclosure of information during medical treatment does not automatically authorize every subsequent use of that information. Nissenbaum argues that privacy depends upon the appropriateness of information flows within particular social contexts rather than on absolute secrecy (Nissenbaum 2010). The healthcare context establishes expectations concerning who may receive information, for what purpose, and under what conditions. A patient who communicates with a physician therefore enters a particular informational context characterized by therapeutic purpose and professional confidentiality. The subsequent transfer of that information into a recording, cloud repository, educational database, or artificial-intelligence system may constitute a new information flow requiring independent justification. From this perspective, unauthorized recording is problematic because it changes the informational context without necessarily obtaining the patient's agreement to that change.

The concept of informational autonomy further clarifies the relationship between privacy and informed consent. Patient autonomy is not exhausted by the right to accept or refuse medical treatment; it also concerns the patient's ability to participate meaningfully in decisions about the handling of information generated through healthcare. Beauchamp and Childress characterize respect for autonomy as requiring conditions that enable individuals to make intentional and adequately informed decisions (Beauchamp and Childress 2019). In digital healthcare, those conditions include understanding whether a consultation is recorded, the reason for recording, the identity of those who may access it, and the possible duration and scope of subsequent use. Research concerning digital-health ethics similarly identifies autonomy, consent, transparency, accountability, privacy, and fairness as interconnected governance principles (Keenan, Tsourtos, and Tieman 2021; Vayena, Blasimme, and Cohen 2018).

The persistence of digital information creates another important conceptual distinction between communication and documentation. Traditional clinical documentation involves selective recording of information considered relevant to treatment. An audiovisual recording can capture substantially more information than is clinically necessary. It may therefore violate data-minimization principles even when the underlying medical consultation was lawful. Research on electronic health records has shown that privacy risks are associated not only with external cybersecurity threats but also with internal access, documentation practices, inadequate governance, and uncertainty regarding how information is subsequently used (Keshta and Odeh 2013; Alhuwail et al. 2020). Recording an entire consultation consequently requires justification that goes beyond the mere technological possibility of preserving the encounter. The relevant legal question is

whether comprehensive recording is necessary and proportionate to the purpose for which it is undertaken.

## Methodology

This research adopts a normative juridical methodology directed toward the interpretation and evaluation of legal norms governing unauthorized recording of online medical consultations. The statutory approach examines Indonesian legal instruments governing health services, personal data protection, medical records, and telemedicine, particularly Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, Minister of Health Regulation Number 24 of 2022 concerning Medical Records, Minister of Health Regulation Number 20 of 2019 concerning Telemedicine Services between Health Facilities, and Government Regulation Number 28 of 2024. The conceptual approach examines privacy, confidentiality, informed consent, autonomy, purpose limitation, data minimization, and accountability. The comparative approach considers international scholarship and regulatory principles concerning telemedicine privacy and health-data governance. This combination is necessary because the legal status of a recording cannot be adequately determined through one regulatory instrument alone.

The secondary literature was selected from peer-reviewed academic journals and authoritative scholarly publications dealing directly or substantially with telemedicine privacy, confidentiality, informed consent, electronic health records, health-data governance, cybersecurity, or the legal and ethical implications of telehealth. The literature includes systematic reviews, empirical studies, legal analyses, and normative scholarship published before 2026. Particular attention was given to studies addressing privacy and security practices in telehealth, audiovisual recording of telehealth encounters, informed consent in digital health, secondary use of health data, and the relationship between patient trust and health-data sharing. The literature was analyzed thematically rather than statistically. The purpose was to identify recurring normative principles and use them to evaluate whether the existing Indonesian framework provides adequate protection against unauthorized recording and secondary use.

## Results and Discussion

### A. The Legal Aspect of Telemedicine Recordings

A telemedicine recording possesses a hybrid legal character because a single digital file may contain several forms of legally protected information simultaneously. It can contain the patient's identity, medical history, symptoms, diagnosis, treatment information, physical appearance, voice, emotional expressions, and information concerning third persons present during the consultation. Under a personal-data framework, much of this information may constitute personal data, while information concerning health falls within a

particularly sensitive category. Under health law, the same content may constitute confidential health information, and where it is incorporated into clinical documentation it may become associated with the medical record. The literature on electronic health records demonstrates that digital health information should not be evaluated merely according to its technological format because the sensitivity and governance requirements depend substantially upon content, purpose, access, and subsequent use (Shenoy and Appel 2017; Watzlaf et al. 2017).

This hybrid character is important because it means that the absence of a specific statutory provision expressly prohibiting "telemedicine recording without consent" does not necessarily create a legal vacuum. Instead, several existing obligations may apply simultaneously. Personal-data law governs processing, while health legislation governs confidentiality and medical information. Medical-record regulation imposes additional obligations when information becomes part of clinical documentation. The Indonesian legal literature increasingly recognizes that telemedicine is governed by a fragmented framework involving health law, personal-data protection, medical-record regulation, and professional obligations (Budiyanti and Herlambang 2021; Andrianto and Athira 2022; Makarim and Wijayanto 2024). The analytical challenge is therefore not simply to identify one applicable statute but to determine how these overlapping regimes collectively restrict the authority of healthcare providers to create and process consultation recordings.

## 1. Recording as an Independent Processing Activity

The central proposition of this article is that recording should be treated as an independent processing activity. This proposition follows from the fact that recording is not merely a passive transmission of information. It creates a persistent representation of an interaction that can be stored, duplicated, searched, transmitted, and analyzed independently of the original consultation. A physician may legitimately receive sensitive information because it is necessary for diagnosis and treatment without necessarily possessing unlimited authority to reproduce that information audiovisually. The distinction resembles the difference between hearing a confidential statement and creating a permanent archive of the statement. Scholarship concerning audiovisual telehealth encounters directly identifies recording as a separate medico-legal issue involving consent, privacy, confidentiality, and medical records (Farmer et al. 2021). The legal characterization should therefore reflect the additional consequences produced by recording rather than treating it as an incidental technological feature.

The independent character of recording also follows from the logic of informed consent. Consent must relate to the decision actually being authorized. If a patient agrees to a video consultation, the immediate object of consent is participation in remote healthcare. Recording creates a further decision because it determines whether the interaction will become a durable digital object. The literature on telemedicine repeatedly emphasizes that informed consent remains

necessary in remote healthcare and that patients should be adequately informed about the limitations and risks of digital communication (Chaet et al. 2017; Nittari et al. 2020). Research on electronic consent further demonstrates that meaningful digital consent requires adequate information and understanding rather than merely an electronic acknowledgment (De Sutter et al. 2020). Consequently, general consent to telemedicine should not be presumed to include authorization for recording unless the recording is clearly disclosed and its purpose is incorporated into the consent process.

## 2. Unauthorized Recording and Patient Privacy

Unauthorized recording should be conceptualized as a privacy interference even when no third-party disclosure subsequently occurs. This position follows from the broader understanding of privacy as encompassing the collection and processing of personal information. If a patient reasonably expects a consultation to remain a confidential interaction, covertly converting the interaction into a permanent audiovisual file changes the conditions under which the patient's information is being processed. Solove's framework is particularly useful because it distinguishes different forms of privacy harm rather than treating privacy solely as secrecy from the public (Solove 2006). The recording may create informational risks that remain invisible to the patient, including internal access, future secondary use, transfer to third parties, or exposure through a security incident. The legal significance therefore lies partly in the unauthorized creation of informational persistence, not merely in later dissemination.

Contextual integrity strengthens this argument by emphasizing that information flows must remain consistent with the norms of the context in which information was originally disclosed (Nissenbaum 2010). The physician–patient relationship establishes strong expectations concerning confidentiality and therapeutic purpose. A patient may reasonably disclose highly sensitive information because the communication occurs within that context. When a provider records the consultation without informing the patient, the provider introduces a new form of information flow that was not necessarily contemplated by the patient. The problem is therefore not simply that the patient “shared” information voluntarily. Rather, the patient shared information under a particular contextual expectation. Transforming that information into an enduring audiovisual record may exceed the informational norms associated with the original disclosure. Unauthorized recording consequently raises a distinct autonomy and privacy concern even if the file remains technically secure.

## 3. Medical Confidentiality and the Physician–Patient Relationship

Medical confidentiality represents more than a rule concerning nondisclosure; it is a structural condition of trust that enables patients to communicate honestly with healthcare professionals. The literature on telemedicine identifies confidentiality as one of the foundational ethical and legal principles that must

survive the transition from physical to virtual healthcare (Stanberry 1997; Chaet et al. 2017). Electronic health-record research similarly indicates that patients' confidence in the confidentiality and security of health information affects their willingness to participate in digital healthcare systems (Shenoy and Appel 2017; Papadopoulos, von Wyl, and Gille 2024). The creation of an undisclosed recording can undermine this relationship because patients may reasonably perceive the recording as a departure from the confidentiality they expected. Even when the provider intends no malicious use, the absence of transparency can weaken the trust necessary for effective healthcare communication.

The importance of confidentiality is heightened in telemedicine because patients may participate from private residences rather than controlled clinical environments. The physical setting can introduce additional privacy risks, including other individuals overhearing conversations, unauthorized devices, or insecure networks. Research on telemedicine privacy has demonstrated that privacy risks arise from environmental, technological, and operational factors rather than from cybersecurity alone (Houser, Flite, and Foster 2023). Mishkin et al. similarly emphasize that telemedicine can create unexpected privacy problems arising from the patient's physical surroundings and the difficulty of ensuring genuinely autonomous decision-making in remote environments (Mishkin et al. 2023).

Recording can amplify these risks because it permanently captures circumstances that might otherwise remain temporary. The legal response should therefore recognize privacy as encompassing both technological and contextual dimensions.

## 4. Consent, Autonomy, and Digital Healthcare

The doctrine of informed consent becomes particularly significant when recording is introduced into telemedicine. A valid consent process should communicate the material implications of the decision in a manner that permits meaningful choice. This requirement cannot be satisfied merely by embedding a recording clause within extensive platform terms and conditions that patients are unlikely to read or understand. Studies of electronic informed consent demonstrate that comprehension, usability, security, legal validity, and transparency remain significant challenges in digital environments (De Sutter et al. 2020). Tully et al. similarly argue that connected medical technologies require a broader conception of informed consent that accounts for cybersecurity and technological risks affecting patient autonomy (Tully et al. 2020).

A patient-centered approach consequently requires differentiation between necessary and optional recording. If a recording is genuinely necessary to provide a particular healthcare service, the provider should explain why recording is necessary and what consequences follow from it. If recording is merely convenient for quality assurance, training, or institutional purposes, refusal should ordinarily not result in denial of healthcare. Otherwise, the apparent consent may be influenced by the structural inequality between provider and patient. The literature

on telehealth ethics identifies autonomy, professional–patient relationships, privacy, and confidentiality as interconnected concerns, while systematic review evidence indicates that autonomy is among the most frequently discussed ethical principles in telehealth scholarship (Keenan, Tsourtos, and Tieman 2021).

## 5. Data Minimization and Necessity

The principle of data minimization provides an important limitation on routine recording. A healthcare provider should collect and retain only information reasonably necessary for a legitimate purpose. An entire video consultation may contain substantially more information than is needed for clinical documentation. For example, a patient's background environment, facial expressions, family conversations, or incidental statements may have no clinical relevance. Recording all of these elements creates additional privacy exposure without necessarily improving treatment. Research on health-information technologies repeatedly emphasizes the importance of limiting information collection and implementing appropriate governance mechanisms (Watzlaf et al. 2017; LaMonica et al. 2021).

Necessity should therefore be assessed before recording begins rather than assumed from technological availability. The question should be whether the healthcare objective can reasonably be achieved through a less intrusive mechanism, such as written clinical notes, selective documentation, or temporary technical recordings. The principle is especially relevant because digital storage is inexpensive and platforms may make recording technically effortless. Convenience, however, should not become a substitute for legal necessity. If a provider can achieve the same legitimate objective without creating a comprehensive audiovisual archive, recording the entire consultation may be disproportionate. A rights-centered interpretation of data protection therefore requires the provider to justify both the decision to record and the extent of information captured.

## 6. Retention and the Persistence of Digital Medical Information

The privacy risk associated with recording does not end when the consultation is completed. Retention creates a continuing legal and ethical relationship between the patient and the recording. Every additional day that a recording remains stored creates another period during which unauthorized access, accidental disclosure, cyberattack, or secondary use may occur. Research on telehealth privacy practices identifies retention as an important element of privacy governance alongside access control, authentication, encryption, and confidentiality (Watzlaf et al. 2017). Broader research on electronic health records similarly demonstrates that security risks can arise from unauthorized internal access, inadequate auditing, and weak organizational practices rather than exclusively from external attacks (Alhuwail et al. 2020).

Retention should consequently be linked to the original purpose for which the recording was created. A recording that forms part of legitimate clinical documentation may be subject to medical-record requirements, whereas a

temporary technical recording should ordinarily have a substantially shorter retention period. Educational and research recordings may require distinct retention policies based on their specific purposes and ethical approvals. Indefinite retention should not become the default merely because storage capacity is available. Such a practice would effectively transform healthcare institutions into permanent custodians of patients' audiovisual medical histories. A proportionate system should determine the retention period in advance, communicate it to the patient, restrict access during the retention period, and employ automated deletion mechanisms where appropriate.

## 7. Secondary Use and Function Creep

Secondary use represents one of the most important risks associated with telemedicine recordings because the informational value of a recording extends far beyond the original consultation. A recording created for clinical purposes might subsequently be useful for medical education, physician training, research, artificial-intelligence development, speech recognition, quality assessment, or commercial analytics. The movement from one purpose to another creates a risk of function creep, whereby information collected in one context gradually becomes available for unrelated objectives. Research on secondary use of health information demonstrates that privacy, transparency, trust, and consent significantly influence public attitudes toward health-data sharing (Hutchings et al. 2020; Richter et al. 2021).

The problem is particularly acute where identifiable audiovisual recordings are used for research or artificial-intelligence development. A recording may contain not only explicit medical information but also biometric and behavioral characteristics that make effective anonymization difficult. Secondary-use research therefore emphasizes the importance of consent, governance, institutional review, transparency, and proportionality when clinical data are reused (Mezinska et al. 2020; Zenker et al. 2022). The fact that a patient initially consented to treatment cannot automatically establish that the patient consented to all future uses of the recording. Each additional purpose should be assessed according to its relationship to the original purpose, the sensitivity of the information, the identity of subsequent users, and the safeguards available to prevent inappropriate use.

## 8. Electronic Medical Records and Consultation Recordings

A further issue concerns whether a telemedicine recording automatically becomes part of the medical record. A categorical approach would be problematic because audiovisual recordings may contain substantially more information than is necessary for clinical documentation. Medical records traditionally involve selective documentation of information relevant to diagnosis, treatment, and continuity of care. A full consultation recording may contain personal or contextual information that has no clinical relevance. Research on electronic health records recognizes the importance of balancing information availability against

confidentiality and patient control (Keshta and Odeh 2013; Shenoy and Appel 2017). Consequently, the legal status of a recording should be determined functionally rather than solely according to the fact that it was generated during a healthcare encounter.

Where a recording is intentionally retained as evidence of clinical assessment or forms an integral part of clinical decision-making, the relevant content may need to be governed within the medical-record framework. Where a recording is created for a temporary technical purpose, however, it may be subject to a different retention and access regime. This distinction should not be interpreted as removing privacy protection from temporary recordings. Rather, it recognizes that different purposes justify different governance requirements. The central principle should be that the provider must identify the function of the recording at the moment of creation and ensure that subsequent retention and use remain consistent with that function. This approach is more consistent with purpose limitation than treating every digital file as an undifferentiated medical record.

## 9. Responsibility of Healthcare Providers and Platforms

Telemedicine frequently involves multiple actors, including physicians, hospitals, platform operators, cloud-storage providers, software developers, and other technology vendors. This creates a complex distribution of technical access and legal responsibility. The existence of a third-party platform should not, however, allow healthcare providers to avoid responsibility for the consequences of recording. Literature concerning telemedicine governance emphasizes that clearly defined responsibilities among stakeholders are necessary to establish trust and manage legal risk (Amith et al. 2018; Nittari et al. 2020). The provider should therefore understand which entities process recordings, for what purposes, under what contractual arrangements, and with what security controls.

The appropriate principle is organizational accountability. Healthcare institutions should determine whether recording is permitted, identify legitimate purposes, establish consent procedures, define retention periods, restrict access, and monitor compliance. Technology vendors should be contractually bound to process recordings only within authorized purposes and should implement appropriate security measures. Research on telehealth privacy practices identifies access control, authentication, encryption, confidentiality, availability, and retention as interconnected elements of responsible governance (Watzlaf et al. 2017). A provider that simply delegates storage to a cloud service should therefore not assume that the delegation eliminates its own obligations. Technological outsourcing changes the mechanism of processing but should not eliminate the underlying duty to protect patients.

Cybersecurity and Privacy by Design

Cybersecurity is essential to protecting telemedicine recordings, but security should not be confused with privacy. A recording may be securely encrypted and

still have been created unlawfully. Conversely, a recording may have been legitimately created but subsequently compromised because of inadequate technical controls. The literature on telemedicine security demonstrates that security problems involve confidentiality, integrity, authentication, access control, and the adequacy of technical standards (Garg and Brewer 2011). Research on secure telemedicine systems similarly emphasizes anonymity, confidentiality, integrity, authentication, and secure data transmission as critical components of digital healthcare infrastructure (Rezaeibagha and Mu 2018).

Privacy by design therefore requires both legal and technological controls. Recording should not automatically be activated simply because a platform has the technical capability to do so. Patients should receive a visible indication whenever recording occurs, while access should be restricted according to professional necessity. Audit logs should identify who accessed the recording and when, while downloading or external transfer should be subject to additional authorization. Encryption should protect stored and transmitted data, but deletion mechanisms are equally important because unnecessary retention increases exposure. The broader literature on digital-health governance supports the integration of privacy, security, accountability, and transparency rather than treating cybersecurity as an isolated technical issue (Vayena, Blasimme, and Cohen 2018; LaMonica et al. 2021).

## 10. Exceptions to Confidentiality

Medical confidentiality is not absolute. Healthcare law recognizes circumstances in which disclosure may be justified by law enforcement, public health, protection of others, healthcare needs, patient requests, or other legally recognized purposes. Nevertheless, an exception permitting disclosure should not automatically be transformed into a general authority to record consultations. Disclosure and recording are distinct activities. A legal rule may permit access to an existing medical record under specified circumstances without authorizing healthcare providers to routinely create comprehensive recordings in anticipation of potential future requests. This distinction is particularly important because an exception to confidentiality should be interpreted in accordance with its specific purpose rather than expanded into a general exception to patient autonomy.

The same reasoning applies to research and education. A legitimate research objective does not necessarily justify collecting identifiable audiovisual recordings when the research can be performed using de-identified or less intrusive information. Literature on secondary health-data use emphasizes that public interest, anonymization, consent, ethics review, and proportionality must be evaluated together (Mezinska et al. 2020). The existence of an educational or research exception should therefore not eliminate the requirement to assess necessity and proportionality. The appropriate principle is that exceptions to confidentiality may justify particular information flows but should not create an unlimited power to create and preserve new information assets. This interpretation better reconciles patient autonomy with legitimate institutional and public interests.

## 11. Patient Trust and Health Justice

Patient privacy is also connected to trust, which is fundamental to the sustainability of digital healthcare. Empirical research indicates that trust in healthcare providers can influence patients' willingness to share personal health information and participate in electronic health-record systems (Cherif, Bezaz, and Mzoughi 2021). A privacy framework that fails to reassure patients may therefore undermine one of the conditions necessary for successful digital-health adoption. Trust is particularly important in telemedicine because patients must disclose information through technological systems that they may not fully understand. If patients discover that consultations have been recorded without their knowledge, they may become less willing to disclose sensitive information in future consultations. This could have consequences not only for privacy but also for diagnostic accuracy and continuity of care.

The issue also raises questions of health justice. Telemedicine is frequently promoted as a mechanism for expanding access to healthcare for geographically isolated or underserved populations. However, the benefits of accessibility should not be achieved by transferring disproportionate privacy risks to patients who have limited alternatives. Research on telemedicine identifies unequal technological access and privacy concerns as important barriers to equitable digital healthcare (Dash, Aarthy, and Mohan 2021; Keenan, Tsourtos, and Tieman 2021). Patients should not have to choose between receiving healthcare and surrendering control over highly sensitive information. Privacy should therefore be treated as part of equitable healthcare access rather than as an optional privilege.

## B. Indonesian Legal Framework

The Indonesian Personal Data Protection Law provides an important foundation for regulating telemedicine recordings because health data and information are classified as specific personal data. This classification recognizes that processing health information creates heightened risks for individuals. The significance of this provision is that the legal analysis begins at the point of processing rather than only when information is disclosed. Recording a consultation necessarily involves processing because information is captured and transformed into a stored digital representation. Consequently, healthcare providers should identify the applicable legal basis, purpose, scope, recipients, retention period, and security measures before recording occurs. Indonesian legal scholarship has identified the PDP Law as a central component of the regulatory architecture applicable to patient data in telemedicine, although questions concerning coordination with sector-specific health regulations remain significant (Jannah, Amboro, and Shahrullah 2024).

Law Number 17 of 2023 concerning Health adds a distinct confidentiality dimension. The Health Law recognizes the patient's right to confidentiality of personal health data and information and establishes circumstances in which

confidentiality may be limited. This is significant because health information is not merely an ordinary category of personal data; it is embedded within a professional relationship in which patients disclose information because they expect it to be protected. The Health Law should therefore be interpreted together with the PDP Law rather than as an alternative regime. The former emphasizes health-related confidentiality and patient rights, while the latter provides a broader framework for personal-data processing. The combination supports a cumulative interpretation under which telemedicine providers must satisfy both health-sector confidentiality requirements and personal-data governance obligations.

Minister of Health Regulation Number 24 of 2022 concerning Medical Records provides another important component of the framework. The regulation reflects the transition toward electronic medical records and emphasizes the need for security and confidentiality in the management of health information. The relevance of the regulation to telemedicine recordings depends on whether and how the recording becomes part of the medical record. It should not be assumed that every audiovisual recording is automatically equivalent to a medical record. Instead, the regulatory status should depend on the purpose and function of the recording and whether it constitutes documentation necessary for clinical care. The literature on electronic health records supports this functional approach because it recognizes that the availability and portability of digital information create both clinical benefits and confidentiality risks (Keshta and Odeh 2013; Shenoy and Appel 2017).

Government Regulation Number 28 of 2024 strengthens the implementation of the Health Law and provides additional rules concerning medical records and confidentiality. Its significance for telemedicine is that it reinforces the proposition that health information must remain subject to confidentiality even when healthcare processes become digitally mediated. The regulation should therefore be interpreted alongside the PDP Law to create an integrated governance framework. However, the existing framework remains insufficiently specific concerning the recording of live telemedicine consultations. It does not clearly establish whether recording should always require separate consent, how long recordings should be retained, or when a recording may be reused for education, research, or artificial-intelligence development. This regulatory uncertainty supports the need for a more explicit interpretive framework centered on purpose, necessity, consent, and patient autonomy.

## C. Comparative Analysis

The European data-protection framework provides a useful comparative reference because it recognizes health information as particularly sensitive and subjects its processing to heightened requirements. The GDPR also emphasizes principles such as purpose limitation, data minimization, transparency, accountability, and lawful processing. These principles are valuable for interpreting telemedicine recording because they demonstrate that privacy protection concerns

the entire processing lifecycle rather than only the final disclosure of information. Indonesian law should not simply replicate the GDPR, particularly because the legal and institutional contexts differ. Nevertheless, the underlying principles can provide persuasive comparative guidance. The Indonesian literature comparing the PDP Law and GDPR similarly identifies substantial convergence concerning consent, patient rights, security, and restrictions on disclosure to third parties (Jannah, Amboro, and Shahrullah 2024).

The comparative literature also demonstrates that consent should become more specific as the sensitivity and intrusiveness of processing increase. The use of a consultation recording for direct patient care is conceptually different from its use for research or commercial development. Research concerning secondary use of health information shows that patients may support data sharing when transparency and governance safeguards are present but may become concerned when the purpose and recipients are unclear (Hutchings et al. 2020). Studies of patient attitudes toward secondary research use similarly demonstrate that consent and public trust are central to the legitimacy of health-data reuse (Richter et al. 2021). These findings support an approach in which the legal validity of recording depends not only on whether the provider has a legitimate purpose but also on whether the patient has sufficient information concerning that purpose and the future life of the recording.

## D. Proposed Governance Model

The analysis supports a consent-centered governance model in which recording is treated as a distinct processing activity subject to a clearly defined legal and ethical framework. The model begins with prior disclosure because patients cannot make meaningful choices concerning recording if they do not know that recording will occur. The disclosure should explain the nature of the recording, its purpose, the responsible organization, the expected retention period, the categories of persons who may access it, and any foreseeable secondary uses. This approach is consistent with research on telehealth privacy and electronic informed consent, which emphasizes transparency and understanding as essential components of legitimate digital-health practices (Watzlaf et al. 2017; De Sutter et al. 2020).

The second element is specific consent where consent constitutes the applicable legal basis. Consent to receive telemedicine should be conceptually separated from consent to recording. The patient should be able to understand that participation in the consultation and authorization of recording are distinct decisions. Where recording is unnecessary for treatment, the patient should ordinarily be permitted to refuse recording without losing access to healthcare. This approach protects against coercive consent arising from the structural imbalance between healthcare providers and patients. It is also consistent with the broader ethical literature identifying autonomy as a central principle of telehealth governance (Keenan, Tsourtos, and Tieman 2021). The purpose is not to create

unnecessary administrative burdens but to ensure that technological convenience does not silently expand the scope of patient authorization.

The third element is strict purpose limitation. A recording should be used only for the purpose communicated when it was created unless another valid legal basis authorizes subsequent processing. A recording created for clinical documentation should not automatically become an institutional resource for unrelated education, research, marketing, or artificial-intelligence development. Secondary use should be independently assessed according to necessity, compatibility, sensitivity, and safeguards. Scholarship on health-data sharing demonstrates that transparency and governance significantly influence public attitudes toward secondary use (Hutchings et al. 2020; Richter et al. 2021). The principle is particularly important for audiovisual data because recordings can contain information that is difficult to anonymize completely. Purpose limitation therefore protects patients against function creep while still allowing legitimate research and innovation under appropriately governed conditions.

The fourth element is data minimization and retention limitation. Providers should record only what is reasonably necessary and should retain recordings only for as long as the relevant purpose requires. Full-session audiovisual recording should not become routine where selective documentation can achieve the same clinical objective. Retention periods should be established in advance and should correspond to the function of the recording. Technical recordings created temporarily for quality control should not automatically be subject to the same retention period as clinical documentation. This approach follows the broader privacy literature emphasizing that data security depends not only upon encryption but also upon limiting the amount and duration of stored information (Garg and Brewer 2011; Watzlaf et al. 2017).

The fifth element is access restriction and accountability. Telemedicine recordings should be accessible only to persons whose professional responsibilities require access. Role-based permissions, authentication, encryption, audit logs, and restrictions on downloading or external transfer should form part of the technological architecture. Research on electronic health records indicates that unauthorized internal access and weak organizational practices can represent significant threats to confidentiality (Alhuwail et al. 2020). The legal obligation should therefore extend beyond the physician to the healthcare institution and relevant technology providers. Every access event should be traceable, allowing the institution to identify inappropriate use and demonstrate compliance. Accountability transforms privacy from an abstract principle into an operational obligation.

The final element is effective patient remedy. Patients should have a practical mechanism to discover whether a consultation was recorded, understand the purpose of processing, exercise applicable data rights, report unauthorized recording, and seek corrective action when their information has been misused. A legal framework that recognizes privacy rights without providing accessible

remedies remains incomplete. Research on patient trust in electronic health systems demonstrates that transparency and confidence in governance affect willingness to participate in digital information systems (Cherif, Bezaz, and Mzoughi 2021). Effective remedies therefore serve not only compensatory functions but also preventive functions because they create incentives for healthcare providers and platforms to establish stronger privacy practices.

## E. Legal and Policy Implications

The principal regulatory implication is the need for Indonesia to develop clearer standards concerning telemedicine recording. Existing health and personal-data legislation provides a substantial normative foundation, but the specific issue of recording remains dispersed across broader rules concerning confidentiality, personal data, and medical records. A dedicated provision or authoritative regulatory guidance could clarify when recording is permitted, when specific consent is necessary, how recordings should be classified, what retention standards apply, and which secondary uses require separate authorization. Such a framework should be technology-neutral so that it remains relevant as telemedicine platforms evolve. The objective should not be to prohibit recording but to ensure that recording is connected to legitimate purposes and governed throughout its lifecycle.

The regulatory framework should also distinguish between legally necessary recording and institutionally convenient recording. Where recording is essential to a particular healthcare process, the provider should demonstrate necessity and inform the patient of the consequences. Where recording is optional, the patient should be free to refuse without being denied access to appropriate healthcare. This distinction is necessary because the healthcare relationship is characterized by asymmetry: patients depend upon providers for medical assistance and may therefore feel compelled to accept technological practices they would otherwise reject. Treating every electronic acceptance as meaningful consent risks overlooking this structural context. The literature on telehealth ethics supports the importance of autonomy, patient empowerment, and professional responsibility in digital healthcare (Keenan, Tsourtos, and Tieman 2021).

The policy framework should additionally establish clear rules concerning secondary use. Recordings created for clinical care should not automatically be available for research, education, artificial-intelligence development, or commercial analytics. Where secondary use is legitimate, providers should determine whether identifiable recordings are necessary or whether de-identification can adequately achieve the intended purpose. Where identifiable data remain necessary, stronger governance should apply, including appropriate consent, ethics review where applicable, access restrictions, retention limits, and transparency. The literature on secondary health-data use strongly supports the importance of trust, transparency, consent, and governance in determining public acceptance of data sharing (Hutchings et al. 2020; Mezinska et al. 2020).

## Conclusion

Unauthorized recording of online medical consultations represents a distinct privacy problem that cannot be adequately addressed by focusing solely on subsequent disclosure or cybersecurity. Recording transforms a temporary medical interaction into a persistent digital information asset containing potentially sensitive health, biometric, behavioral, and contextual information. The legal significance of this transformation lies in the creation and continued processing of the recording itself. International scholarship has consistently demonstrated that telemedicine creates distinctive challenges concerning privacy, confidentiality, informed consent, security, and professional responsibility, while specific medico-legal research on audiovisual telehealth recordings confirms that recording raises independent questions concerning consent and medical records (Farmer et al. 2021; Nittari et al. 2020).

The Indonesian regulatory framework already provides important protection through personal-data protection law, health law, medical-record regulation, and telemedicine regulation. Nevertheless, the existing framework does not sufficiently articulate the specific relationship between telemedicine consent and recording authorization. This article therefore proposes that recording should generally be treated as an independent processing activity. Consent to receive medical care through telemedicine should not automatically be interpreted as consent to record the consultation. Where consent is the applicable legal basis, authorization should be specific, informed, voluntary, and demonstrable. Where another legal basis exists, the provider should nevertheless establish necessity, proportionality, transparency, and appropriate safeguards.

The proposed consent-centered governance model further requires purpose limitation, data minimization, defined retention periods, restricted access, technical security, accountability, controlled secondary use, and effective patient remedies. Such an approach recognizes that privacy protection must begin before recording occurs and continue throughout the information lifecycle. It also recognizes that cybersecurity, although essential, cannot cure an unlawful collection practice. A securely stored recording may still violate patient autonomy if it was created without legitimate authorization. Conversely, valid authorization does not eliminate the provider's obligation to protect the recording against unauthorized access or misuse.

The broader implication is that telemedicine should not be permitted to weaken the normative foundations of medical confidentiality. Technological innovation should enhance healthcare access and quality without transforming patient vulnerability into an institutional entitlement to collect and retain more information than is necessary. Protecting privacy in telemedicine is therefore not simply a matter of compliance with personal-data legislation. It is an expression of patient autonomy, professional confidentiality, trust, dignity, and health justice. A sustainable digital-health system must ensure that patients can seek healthcare

without being required to surrender control over the intimate information generated during their medical consultations.

## References


Alhuwail, Dhiyaa, Mowafa Househ, Khalid El Kheir, and others. 2020. "Privacy, Confidentiality, Security and Patient Safety Concerns about Electronic Health Records." *International Nursing Review* 67. https://doi.org/10.1111/inr.12585.

Amith, M. T., R. A. K. P. K. Tao, M. R. J. Z. etc. 2018. "Trusting Telemedicine: A Discussion on Risks, Safety, Legal Implications and Liability of Involved Stakeholders." *International Journal of Medical Informatics* 112: 90–98. https://doi.org/10.1016/j.ijmedinf.2018.01.012.

Andrianto, W., and A. B. Athira. 2022. "Telemedicine (Online Medical Services) dalam Era New Normal Ditinjau Berdasarkan Hukum Kesehatan." *Jurnal Hukum & Pembangunan* 52 (1). https://doi.org/10.21143/jhp.vol52.no1.3331.

Bassan, Sharon. 2020. "Data Privacy Considerations for Telehealth Consumers amid COVID-19." *Journal of Law and the Biosciences* 7 (1): lsaa075. https://doi.org/10.1093/jlb/lsaa075.

Budiyanti, Rani Tiyas, and Penggalih Mahardika Herlambang. 2021. "Perlindungan Hukum Pasien dalam Layanan Konsultasi Kesehatan Online." *Jurnal Hukum Kesehatan Indonesia* 1 (1). https://doi.org/10.53337/jhki.v1i01.1.

Chaet, Danielle, Ron Clearfield, James E. Sabin, and Kathryn Skimming. 2017. "Ethical Practice in Telehealth and Telemedicine." *Journal of General Internal Medicine* 32 (10): 1136–1140. https://doi.org/10.1007/s11606-017-4082-2.

Cherif, Emna, Nora Bezaz, and Manel Mzoughi. 2021. "Do Personal Health Concerns and Trust in Healthcare Providers Mitigate Privacy Concerns? Effects on Patients' Intention to Share Personal Health Data on Electronic Health Records." *Social Science & Medicine* 277: 114146. https://doi.org/10.1016/j.socscimed.2021.114146.

Dash, Sambit, Ramasamy Aarthy, and Viswanathan Mohan. 2021. "Telemedicine during COVID-19 in India—A New Policy and Its Challenges." *Journal of Public Health Policy* 42: 501–509. https://doi.org/10.1057/s41271-021-00287-w.

De Sutter, Evelien, Drieda Zaze, Stefania Boccia, Maria Luisa Di Pietro, David Geerts, Pascal Borry, and Isabelle Huys. 2020. "Implementation of Electronic Informed Consent in Biomedical Research and Stakeholders' Perspectives: Systematic Review." *Journal of Medical Internet Research* 22 (10): e19129. https://doi.org/10.2196/19129.

Dorsey, E. Ray, Michael S. Okun, and Bastiaan R. Bloem. 2020. "Care, Convenience, Comfort, Confidentiality, and Contagion: The 5 C's That Will

Shape the Future of Telemedicine." *Journal of Parkinson's Disease* 10 (3): 893–897. https://doi.org/10.3233/JPD-202109.

Farmer, C. C., S. C. Pang, D. Kevat, J. Dean, D. Panaccio, and P. D. Mahar. 2021. "Medico-Legal Implications of Audiovisual Recordings of Telehealth Encounters." *Medical Journal of Australia* 214: 357–359.e1. https://doi.org/10.5694/mja2.51008.

Garg, Vaibhav, and Jeffrey Brewer. 2011. "Telemedicine Security: A Systematic Review." *Journal of Diabetes Science and Technology* 5 (3): 768–777. https://doi.org/10.1177/193229681100500331.

Houser, Shannon H., Cathy A. Flite, and Susan L. Foster. 2023. "Privacy and Security Risk Factors Related to Telehealth Services—A Systematic Review." *Perspectives in Health Information Management*.

Hutchings, Elizabeth, Max Loomes, Phyllis Butow, and Frances M. Boyle. 2020. "A Systematic Literature Review of Health Consumer Attitudes towards Secondary Use and Sharing of Health Administrative and Clinical Trial Data: A Focus on Privacy, Trust, and Transparency." *Systematic Reviews* 9: 235. https://doi.org/10.1186/s13643-020-01481-9.

Jalali, Mohammad S., Adam Landman, and William J. Gordon. 2021. "Telemedicine, Privacy, and Information Security in the Age of COVID-19." *Journal of the American Medical Informatics Association* 28 (3): 671–672. https://doi.org/10.1093/jamia/ocaa310.

Jannah, Miftahul, F. Yudhi Priyo Amboro, and Rina Shahrullah. 2024. "Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law." *Journal of Law and Policy Transformation* 8 (2).

Keenan, Amanda Jane, George Tsourtos, and Jennifer Tieman. 2021. "The Value of Applying Ethical Principles in Telehealth Practices: Systematic Review." *Journal of Medical Internet Research* 23 (3): e25698.

Keshta, Isam, and Samia Odeh. 2013. "Security and Privacy of Electronic Health Records: Concerns and Challenges." *Egyptian Informatics Journal* 14.

Kuziemsky, Craig E., Shashi B. Gogia, Mowafa Househ, Carolyn Petersen, and others. 2018. "Balancing Health Information Exchange and Privacy Governance from a Patient-Centred Connected Health and Telehealth Perspective." *Yearbook of Medical Informatics* 27 (1): 48–54. https://doi.org/10.1055/s-0038-1641195.

LaMonica, Haley M., Anna E. Roberts, Grace Yeeun Lee, Tracey A. Davenport, and Ian B. Hickie. 2021. "Privacy Practices of Health Information Technologies: Privacy Policy Risk Assessment Study and Proposed Guidelines." *Journal of Medical Internet Research* 23 (9): e26317.

Makarim, Muhammad Haris, and Enggar Wijayanto. 2024. "Telemedicine on the Legal System in Indonesia: Legal Protection of Patients and Health Workers." *Dialogia Iuridica* 16 (1): 27–48. https://doi.org/10.28932/di.v16i1.9422.

Mezinska, Signe, Arnis Buka, Agnese Bankava, and Juris Barzdins. 2020. "Legal and Ethical Issues in Secondary Use of Administrative Health Data: The Case of Latvian Healthcare Monitoring Datalink." *Studies in Health Technology and Informatics* 270: 1138–1142. https://doi.org/10.3233/SHTI200340.

Mishkin, Adrienne D., Jeffrey S. Zabinski, Grayson Holt, and Paul S. Appelbaum. 2023. "Ensuring Privacy in Telemedicine: Ethical and Clinical Challenges." *Journal of Telemedicine and Telecare* 29 (3): 217–221. https://doi.org/10.1177/1357633X221134952.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Nittari, Giulio, Ravjyot Khuman, Simone Baldoni, Graziano Pallotta, Gopi Battineni, Ascanio Sirignano, Francesco Amenta, and Giovanna Ricci. 2020. "Telemedicine Practice: Review of the Current Ethical and Legal Challenges." *Telemedicine and e-Health* 26 (12): 1427–1437. https://doi.org/10.1089/tmj.2019.0158.

Norton, S. A., C. E. Lindborg, and C. B. Delaplain. 1993. "Consent and Privacy in Telemedicine." *Hawaii Medical Journal* 52 (12): 340–341.

Papadopoulos, Kimon, Viktor von Wyl, and Felix Gille. 2024. "What Is Public Trust in National Electronic Health Record Systems? A Scoping Review of Qualitative Research Studies from 1995 to 2021." *DIGITAL HEALTH*.

Rezaeibagha, Fatemeh, and Yi Mu. 2018. "Practical and Secure Telemedicine Systems for User Mobility." *Journal of Biomedical Informatics* 78: 24–32. https://doi.org/10.1016/j.jbi.2017.12.011.

Richter, Gesine, Christoph Borzikowsky, Wiebke Lesch, Sebastian C. Semler, Eline M. Bunnik, Alena Buyx, and Michael Krawczak. 2021. "Secondary Research Use of Personal Medical Data: Attitudes from Patient and Population Surveys in The Netherlands and Germany." *European Journal of Human Genetics* 29: 495–502. https://doi.org/10.1038/s41431-020-00735-3.

Shenoy, Akhil, and Jacob M. Appel. 2017. "Safeguarding Confidentiality in Electronic Health Records." Cambridge Quarterly of Healthcare Ethics 26 (2): 337–341. https://doi.org/10.1017/S0963180116000931.

Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477–560.

Stanberry, B. 1997. "The Legal and Ethical Aspects of Telemedicine. 1: Confidentiality and the Patient's Rights of Access." *Journal of Telemedicine and Telecare* 3 (4): 179–187. https://doi.org/10.1258/1357633971931101.

Tully, Jeffrey, Andrea Coravos, Megan Doerr, and Christian Dameff. 2020. "Connected Medical Technology and Cybersecurity Informed Consent: A New Paradigm." *Journal of Medical Internet Research* 22 (3): e17612. https://doi.org/10.2196/17612.

Vayena, Effy, G. Blasimme, and I. G. Cohen. 2018. "Machine Learning in Medicine: Addressing Ethical Challenges." *PLoS Medicine* 15 (11).

Watzlaf, Valerie J. M., Leming Zhou, Dilhari R. Dealmeida, and Linda M. Hartman. 2017. "A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices Used by Healthcare Providers." *International Journal of Telerehabilitation* 9 (2): 39–59. https://doi.org/10.5195/ijt.2017.6231.

Zenker, Sven, Daniel Strech, Kristina Ihrig, Roland Jahns, Gabriele Mьller, Christoph Schickhardt, Georg Schmidt, Ronald Speer, Eva Winkler, Sebastian Graf von Kielmansegg, and Johannes Drepper. 2022. "Data Protection-Compliant Broad Consent for Secondary Use of Health Care Data and Human Biosamples for (Bio)Medical Research: Towards a New German National Standard." *Journal of Biomedical Informatics* 131: 104096. https://doi.org/10.1016/j.jbi.2022.104096.

**Legal Sources**

Indonesia. 2019. Minister of Health Regulation Number 20 of 2019 concerning the Provision of Telemedicine Services between Health Facilities.

Indonesia. 2022a. Law Number 27 of 2022 concerning Personal Data Protection.

Indonesia. 2022b. Minister of Health Regulation Number 24 of 2022 concerning Medical Records.

Indonesia. 2023. Law Number 17 of 2023 concerning Health.

Indonesia. 2024. Government Regulation Number 28 of 2024 concerning Implementing Regulations of Law Number 17 of 2023 concerning Health.

***

## Acknowledgment
None

## Funding Information
None

## Conflicting Interest Statement
The authors state that there is no conflict of interest in the publication of this article.

## Publishing Ethical and Originality Statement
All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

## Generative AI Statement
N/A