Indonesian Health Justice Review
ISSN: XXXX-XXXXX (Online)
Vol. 3, No. 2, 2026, pp. 119-138
Published online since June 25, 2026

Legal Accountability of Telemedicine Platforms for Medication Errors in Online Healthcare Services

Ajeng Kumala Sari*
Universitas Negeri Semarang, Semarang, Indonesia
ajengkumalasari@students.unnes.ac.id

DOI: https://doi.org/10.65815/qg62zj22

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

*Corresponding Author

Abstract

The rapid expansion of telemedicine has changed the way patients obtain medical consultations and prescriptions. However, medication errors occurring through online healthcare services may involve multiple actors, including physicians, pharmacies, technology platforms, and third-party service providers. This fragmented structure creates uncertainty regarding legal accountability when patients suffer harm from incorrect medication information or prescription-related errors. This article examines the legal responsibility of telemedicine platforms for medication errors arising within digital healthcare services in Indonesia. Using a normative juridical approach, the study analyzes healthcare regulation, professional medical responsibility, consumer protection principles, and platform governance. The analysis demonstrates that existing liability frameworks tend to focus primarily on healthcare professionals while providing less clarity concerning the responsibilities of digital platforms that facilitate, structure, or influence the delivery of healthcare services. The article argues that a platform's responsibility should depend on its functional role rather than merely its formal classification as a technology intermediary. Platforms exercising substantial control over clinical workflows, prescription processes, medication information, or patient communication should bear corresponding duties of safety, transparency, and risk management. A functional accountability model is proposed to strengthen patient protection while maintaining appropriate distinctions between professional medical liability and digital platform responsibility.

[*Perkembangan pesat telemedisin telah mengubah cara pasien memperoleh konsultasi medis dan resep. Namun, kesalahan pengobatan yang terjadi melalui layanan kesehatan daring dapat melibatkan banyak pihak, termasuk dokter, apotek, platform teknologi, dan penyedia layanan pihak ketiga. Struktur yang terfragmentasi ini menciptakan ketidakpastian mengenai pertanggungjawaban hukum ketika pasien menderita kerugian akibat informasi pengobatan yang salah atau kesalahan terkait resep. Artikel ini mengkaji tanggung jawab hukum platform telemedisin atas kesalahan*

pengobatan yang timbul dalam layanan kesehatan digital di Indonesia. Dengan menggunakan pendekatan yuridis normatif, studi ini menganalisis regulasi kesehatan, tanggung jawab medis profesional, prinsip perlindungan konsumen, dan tata kelola platform. Analisis menunjukkan bahwa kerangka kerja pertanggungjawaban yang ada cenderung berfokus terutama pada profesional kesehatan, sementara kurang memberikan kejelasan mengenai tanggung jawab platform digital yang memfasilitasi, menyusun, atau memengaruhi penyampaian layanan kesehatan. Artikel ini berpendapat bahwa tanggung jawab platform harus bergantung pada peran fungsionalnya, bukan hanya klasifikasi formalnya sebagai perantara teknologi. Platform yang menjalankan kendali substansial atas alur kerja klinis, proses resep, informasi pengobatan, atau komunikasi pasien harus memikul kewajiban yang sesuai terkait keselamatan, transparansi, dan manajemen risiko. Sebuah model akuntabilitas fungsional diusulkan untuk memperkuat perlindungan pasien sekaligus mempertahankan perbedaan yang tepat antara tanggung jawab medis profesional dan tanggung jawab platform digital.]

Keywords: Telemedicine, medication errors, digital health platforms, legal liability, patient safety

Introduction

Telemedicine has transformed healthcare delivery by allowing patients to consult physicians, obtain prescriptions, receive medication information, and arrange pharmaceutical delivery without physically entering a conventional healthcare facility. The transformation is particularly significant in geographically dispersed healthcare systems, where digital services can reduce distance, waiting time, and barriers to access. The World Health Organization has recognized telemedicine as a potentially valuable component of health-system strengthening, while emphasizing that its implementation must preserve patient safety, privacy, accountability, traceability, and appropriate professional standards (World Health Organization 2019). Digital healthcare, however, does not eliminate the risks associated with conventional medicine. It redistributes those risks across technological and organizational structures.

Medication errors are an important example. A medication error can arise during prescribing, transcription, dispensing, administration, or monitoring, and may involve an incorrect drug, dose, frequency, route, strength, labeling, or patient. Electronic prescribing has demonstrated potential to reduce some categories of medication error, but research also shows that digital systems can introduce new forms of error and that their effectiveness depends heavily on system design, implementation, and clinical context (Ammenwerth et al. 2008; Roumeliotis et al. 2019). A rapid review of medication safety incidents associated with remote primary care found that electronic prescribing incidents included wrong labels or

instructions and incorrect doses, strengths, or frequencies, demonstrating that digitization changes rather than eliminates medication-safety risks (Mann et al. 2022).

The legal problem becomes more complex when the healthcare service is delivered through a digital platform. In a traditional clinical encounter, the patient, physician, pharmacy, and healthcare institution may be relatively easy to identify. In an online healthcare transaction, the platform may simultaneously function as a communication channel, appointment system, electronic medical-record interface, prescription-management system, medication marketplace, payment intermediary, and logistics coordinator. The platform may also determine how clinical information is displayed to physicians, what medications are searchable, which pharmacies can fulfill prescriptions, how prescription instructions are transmitted, and how patients receive medication information. The platform's functional involvement can therefore be much greater than its formal description as a "technology provider" suggests.

This distinction matters because legal responsibility traditionally follows recognized categories. A physician may be liable for professional negligence. A pharmacist may be responsible for an improper dispensing decision. A hospital or healthcare facility may bear institutional responsibility for organizational failures. A manufacturer may face product-related liability for defective medicines or devices. But the platform may argue that it merely provides technological infrastructure and should not be treated as a healthcare provider. That argument becomes less persuasive when the platform actively structures the conditions under which medical decisions and medication transactions occur.

Indonesia presents a particularly important regulatory setting for examining this problem. The country's healthcare system has moved rapidly toward digital delivery, while its legal framework has developed incrementally. Permenkes No. 20 of 2019 regulates telemedicine between healthcare facilities and remains in force, but its scope does not by itself provide a comprehensive liability framework for contemporary direct-to-consumer telemedicine platforms. The Ministry of Health subsequently developed the broader concept of telehealth and telemedicine within the implementation framework of Law No. 17 of 2023 concerning Health, with Government Regulation No. 28 of 2024 providing more extensive regulation concerning healthcare services, health facilities, health information systems, pharmaceuticals, medical devices, and health technology.

The regulatory landscape therefore contains relevant legal principles but does not yet provide a complete platform-liability doctrine. Law No. 17 of 2023 establishes patient rights, professional responsibilities, patient safety, healthcare-facility obligations, and mechanisms for professional complaints and disputes. Government Regulation No. 28 of 2024 expands the implementation framework for health technology and healthcare services. At the same time, Law No. 8 of 1999 concerning Consumer Protection remains applicable to consumer transactions and imposes obligations concerning safety, information, and responsibility for goods

and services. Electronic-system obligations under Government Regulation No. 71 of 2019 are also relevant because digital platforms must operate reliable and secure electronic systems and remain responsible for the operation of those systems, subject to statutory exceptions.

The problem is consequently not simply that Indonesia lacks a rule stating who is liable for a telemedicine medication error. The deeper problem is that conventional legal categories may fail to capture a platform whose influence crosses the boundary between technology and healthcare. If the platform merely transmits a physician's prescription without modifying it, imposing responsibility for the physician's clinical judgment would be excessive. If, however, the platform automatically substitutes a medication, suppresses warnings, ranks available drugs, alters prescription information, or controls communication between the physician and pharmacy, treating the platform as legally irrelevant would be equally problematic.

This article argues that the appropriate legal approach is a functional accountability model. The platform's liability should depend on what it actually does, what risks it controls, what information it possesses, and what preventive measures it could reasonably implement. Formal contractual labels should not determine substantive responsibility. A platform that exercises substantial operational control over medication-related decisions should bear corresponding duties of safety and risk management, even if its corporate terms describe it merely as a technology intermediary.

The article employs normative juridical research, examining Indonesian legislation and regulatory materials together with international guidance and scholarship on telemedicine, medication safety, digital platforms, professional negligence, and technology-related liability. The analysis is doctrinal and conceptual rather than empirical. It seeks to determine how existing Indonesian legal principles can be interpreted to allocate responsibility among physicians, pharmacies, platforms, and other actors when medication errors occur within online healthcare services.

The existing literature has addressed important aspects of this problem. Telemedicine scholarship has examined professional responsibility, patient safety, privacy, and cross-border practice (Parimbelli et al. 2018; Wootton 2012). Medication-safety research has demonstrated both the benefits and unintended consequences of electronic prescribing (Ammenwerth et al. 2008; Roumeliotis et al. 2019). Legal scholarship concerning artificial intelligence and digital healthcare has increasingly emphasized distributed responsibility rather than exclusive physician liability (Cohen and Slottje 2024; Mello and Guha 2024). Yet comparatively less attention has been given to the legal position of telemedicine platforms as functional intermediaries in medication transactions within Indonesia. This article addresses that gap by connecting healthcare liability with platform governance and by proposing a legal test based on functional control rather than formal classification.

Telemedicine Platforms as More Than Technology Intermediaries

The legal characterization of a telemedicine platform should begin with its actual role in the healthcare transaction. The conventional distinction between a healthcare provider and a technology intermediary assumes that technology merely facilitates communication without materially influencing the underlying service. That assumption becomes increasingly difficult to sustain in modern telemedicine.

A contemporary platform may perform numerous functions simultaneously. It may authenticate the patient, collect medical histories, organize symptoms into standardized categories, match patients with physicians, provide clinical prompts, display medication options, transmit prescriptions, connect pharmacies, process payment, communicate dosage instructions, and coordinate delivery. Each function creates a different risk profile. A platform that performs only appointment scheduling occupies a fundamentally different legal position from one that controls the prescription interface through which the physician selects a medication and the patient receives instructions.

The distinction between facilitation and influence is therefore central. A platform should not become legally responsible for professional medical judgment merely because its software enables a consultation. Yet where software design materially structures the clinical process, the platform cannot plausibly characterize every resulting harm as the independent action of the physician.

This problem resembles the broader transformation of healthcare from individual clinical encounters toward complex sociotechnical systems. Patient safety scholarship has long demonstrated that medical errors often result from multiple interacting failures rather than from the conduct of one individual. The "Swiss cheese" model of healthcare safety, for example, conceptualizes accidents as the alignment of multiple organizational and individual weaknesses rather than as the inevitable product of a single negligent act (Reason 2000). Telemedicine platforms intensify this problem because technology becomes another layer through which clinical information is generated, filtered, transmitted, and acted upon.

Medication errors illustrate the point particularly well. Consider an online consultation in which a physician prescribes a medication at a particular dose. The platform's software automatically displays a different strength because that strength is more readily available through its affiliated pharmacy. If the patient receives the altered medication without an adequate warning, the resulting harm cannot reasonably be analyzed exclusively as physician negligence. The platform has materially altered the medication pathway.

A similar problem arises when a platform's user interface makes certain medicines highly visible while making alternatives difficult to identify. Although the platform may not formally prescribe medication, its design can influence clinical choices. The legal significance of such influence should depend not on whether the

platform technically "prescribed" the drug but on whether its system materially constrained or shaped the prescribing process.

The same reasoning applies to medication information. Suppose a platform provides a medication database that incorrectly states the dosage range or fails to display a clinically significant contraindication. A physician may rely upon the information when prescribing, while the patient may rely upon the platform's instructions when taking the medication. If the information is materially inaccurate and the platform had the ability to prevent or correct the error, its role cannot be dismissed as purely technological.

This is why functional classification is superior to formal classification. A platform's legal obligations should correspond to the functions it performs. A neutral communication service may have relatively limited obligations concerning clinical judgment. A platform that structures clinical workflows and medication transactions should have substantially greater obligations.

Government Regulation No. 71 of 2019 supports this functional approach at the level of electronic-system governance. The regulation requires electronic-system providers to operate systems reliably and securely and provides that providers are responsible for the operation of their electronic systems. It also requires risk management, governance policies, work procedures, and periodic audit mechanisms. These provisions are significant because they establish that digital-system responsibility does not disappear simply because a service is delivered through software.

The relevance of this principle to telemedicine is straightforward. If a platform is an electronic-system provider, its responsibility for the operation of its system should extend to foreseeable risks created by the way that system structures healthcare transactions. The platform should not necessarily become liable for every medical outcome, but it should be responsible for failures within the system functions it controls.

This approach also fits the WHO's conception of safe telemedicine. WHO guidance emphasizes patient safety, privacy, traceability, accountability, consent, and security as conditions for responsible telemedicine implementation (World Health Organization 2019). Traceability is particularly important because online healthcare involves multiple technological and professional actors. Without a clear record of who performed which function, patients may be unable to identify the source of a medication error.

The legal significance of traceability is therefore greater than its technical appearance suggests. A platform should be capable of reconstructing the medication pathway when an incident occurs. The relevant record may include the patient's submitted information, the physician's prescription, any automated system intervention, the medication information displayed to the physician, the pharmacy's dispensing record, patient instructions, and delivery information. Without such an audit trail, platform complexity can become a mechanism for obscuring causation.

The platform's responsibility should consequently increase with its degree of functional integration. The more the platform becomes involved in the substance of healthcare delivery, the weaker the argument becomes that it is merely a passive intermediary.

Medication Errors as Distributed Failures of the Digital Care Pathway

Medication errors should not be conceptualized as a single event occurring at the moment a physician writes a prescription. Medication safety is a process extending from clinical assessment to prescribing, transmission, dispensing, patient communication, administration, and monitoring. Each stage can introduce distinct risks. Research on electronic prescribing illustrates this complexity. Ammenwerth et al. (2008) found substantial reductions in medication errors in many studies following implementation of computerized prescribing systems, but also noted considerable variation in study quality, system design, and outcomes. Roumeliotis et al. (2019) similarly found that electronic prescribing strategies reduced medication and dosing errors in hospital settings, but the evidence was heterogeneous and of very low quality for several outcomes. The lesson is important for legal analysis: digitization may reduce some risks while simultaneously creating different ones.

A legal system that assumes technology is inherently safer than conventional prescribing would therefore be mistaken. The relevant question is whether a particular digital system was reasonably designed, implemented, and supervised for the clinical purpose in which it was used. Medication errors in telemedicine can be divided analytically into several causal stages without converting those stages into rigid legal categories. An error may originate in the clinical assessment, prescription, electronic transmission, medication database, dispensing process, patient instruction, or delivery. The same injury may involve failures at more than one stage.

A physician's liability should generally depend upon the quality of clinical judgment. If the physician diagnoses the patient negligently and prescribes an inappropriate drug despite information that a competent physician should have considered, the existence of a digital platform does not eliminate professional responsibility. Telemedicine changes the medium of care, but it does not eliminate the physician's professional duty.

Yet the physician's responsibility has limits. A physician cannot reasonably be expected to detect every technological alteration of a prescription if the platform silently modifies the information. Nor should a clinician automatically bear responsibility for inaccurate medication information supplied by a platform when the physician had no reasonable basis to suspect that information was incorrect.

The pharmacy occupies another distinct position. Pharmacists may have independent duties to verify prescriptions, identify inappropriate doses, detect contraindications, and dispense medication correctly. A pharmacy that dispenses

the wrong drug or dose despite possessing the relevant prescription and information may therefore bear direct professional responsibility. Conversely, where the platform transmits incorrect information to the pharmacy, the causal contribution of the platform becomes relevant.

The platform occupies the space between these actors. Its responsibility arises when the platform itself creates or materially amplifies the risk. This may occur through defective software, inaccurate medication databases, inadequate prescription-transmission protocols, poor interface design, failure to display clinically significant warnings, unauthorized modification of prescription information, or inadequate controls against foreseeable misuse.

The platform should also bear responsibility where it knowingly creates incentives that increase medication risk. A platform may, for example, prioritize speed over appropriate clinical verification, encourage automated prescription renewal without adequate review, or design workflows that make safety checks practically difficult. In such cases, the problem is not a technical malfunction in the narrow sense. It is a governance failure.

This distinction is important because software may operate exactly as designed while still producing an unsafe outcome. A platform's legal responsibility should not depend entirely on whether a programmer made a coding mistake. If the system was deliberately designed in a way that predictably increases medication risk, the relevant failure is organizational and governance-based.

This perspective is consistent with contemporary patient-safety theory. Reason (2000) emphasizes that organizational systems can create latent conditions that make individual errors more likely. Telemedicine platforms can create similar latent conditions through interface design, workflow architecture, inadequate verification, and insufficient communication among participants.

The rapid review by Mann et al. (2022) is particularly relevant because it identifies medication incidents involving wrong labels, instructions, doses, strengths, and frequencies in electronic prescribing environments. These categories demonstrate that medication safety is partly a communication problem. When a platform controls how medication information is translated from physician to patient, it exercises a function with direct consequences for patient safety. The legal analysis should therefore move beyond the question of who “prescribed” the medicine. Prescription is only one component of medication delivery. If the platform controls the information architecture through which a prescription becomes a medication transaction, it assumes a corresponding duty not to introduce foreseeable safety risks.

This approach also has implications for patient expectations. Patients using a telemedicine platform may reasonably perceive the platform as a unified healthcare service rather than as a collection of legally independent actors. If the platform presents physicians, pharmacies, payment, medication information, and delivery as one integrated service, it may be difficult to justify a legal structure that allows the platform to disaggregate responsibility whenever harm occurs.

The Consumer Protection Law reinforces the importance of this question. Law No. 8 of 1999 remains in force and establishes a general framework for consumer rights, business-actor obligations, and responsibility for goods and services. The law should not automatically be interpreted as converting every healthcare platform into an ordinary seller, because healthcare involves professional duties that cannot be reduced to consumer transactions. Nevertheless, its principles concerning safety, accurate information, and responsible business conduct may supplement healthcare law where the platform directly provides or facilitates consumer-facing services.

The resulting legal picture is therefore layered. Professional medical responsibility governs clinical judgment. Pharmaceutical responsibility governs dispensing. Consumer law can protect users against unsafe or misleading service characteristics. Electronic-system law governs the reliability and security of the technological infrastructure. Health law governs patient safety and healthcare quality. Personal data law governs the processing of health information. The challenge is not to select one regime and exclude the others, but to determine how they interact when a single medication error crosses several regulatory boundaries.

Functional Control as the Basis for Platform Liability

The strongest basis for assigning liability to a telemedicine platform is not contractual proximity to the patient but functional control over the risk that caused the injury. This principle provides a more defensible basis for responsibility because it connects liability to the actor's capacity to prevent harm.

Functional control should be understood broadly. A platform exercises meaningful control when it determines or materially influences how information is collected, processed, displayed, transmitted, or acted upon in the healthcare process. Control may exist even without formal clinical authority.

Consider a platform that merely provides encrypted video communication between a physician and patient. If the physician independently assesses the patient and issues a prescription that is correctly transmitted, the platform's responsibility for a subsequent clinical error should ordinarily be limited. The platform is facilitating communication rather than controlling the medical decision.

The situation changes when the platform automatically structures the consultation. Suppose its software converts patient responses into clinical categories, highlights particular symptoms, suppresses other information, or generates medication suggestions. The platform has then moved closer to the clinical decision-making process. If those functions materially contribute to a medication error, the platform's legal position should reflect its greater influence.

An even stronger case exists where the platform controls prescription selection. If the system automatically substitutes available medication strengths, restricts physicians to a predetermined list, or modifies prescription information before transmission to a pharmacy, it exercises direct operational control over

medication safety. A contractual clause describing the platform as a "technology intermediary" should not shield it from responsibility for risks generated by these functions.

This functional approach is consistent with developments in AI and health law. Cohen and Slottje (2024) and Mello and Guha (2024) emphasize that healthcare technology creates liability questions extending beyond individual clinicians because responsibility may depend on the design, deployment, and use of technological systems. The same logic applies to telemedicine platforms even when AI is not involved.

Functional control also provides a principled distinction between platform liability and professional liability. The physician remains responsible for clinical judgment that falls below the applicable professional standard. The platform becomes responsible for technological or organizational failures within its sphere of control. The pharmacy remains responsible for dispensing activities under its professional obligations. The existence of multiple responsible actors does not mean that responsibility is confused; rather, it means that different duties attach to different functions.

The principle also avoids the opposite danger of excessive platform liability. A platform should not be responsible simply because a patient was harmed after using its service. Medicine inherently involves uncertainty, and not every adverse drug reaction constitutes negligence. If the physician appropriately prescribed a medication, the pharmacy correctly dispensed it, the platform transmitted the prescription accurately, and the patient experienced an unforeseeable adverse reaction, the existence of an adverse outcome should not by itself establish platform liability.

The relevant legal inquiry should instead examine whether the platform breached a duty associated with a risk it could reasonably control. The stronger the platform's control, the stronger the basis for imposing a corresponding duty.

Government Regulation No. 71 of 2019 is especially useful in this regard because it expressly requires electronic-system providers to implement risk management and maintain procedures and audit mechanisms. The regulatory logic is consistent with a risk-control model: an actor responsible for operating a digital system must take reasonable measures against damage or loss arising from that system. The same principle can be connected to Government Regulation No. 28 of 2024. The regulation provides implementing rules concerning healthcare services, healthcare personnel, healthcare facilities, pharmaceuticals and medical devices, health information systems, health technology, and supervision. Although it does not create a comprehensive doctrine specifically addressing telemedicine-platform liability, its broad governance framework supports the proposition that digital health services cannot be legally detached from patient safety.

The platform's contractual structure should therefore be treated as evidence, not as a definitive legal classification. Terms of service may describe a platform as an intermediary, but courts should examine the actual functions performed. A

platform that markets itself as an integrated healthcare service while exercising substantial control over clinical workflows should not be able to invoke its contractual label as an absolute defense.

This is particularly important because platform users ordinarily lack bargaining power and technical knowledge. A patient cannot realistically negotiate the architecture of a digital healthcare platform. Nor can the patient determine whether medication information has been modified by software, whether a prescription was automatically processed, or whether a pharmacy received the exact information entered by the physician. These information asymmetries justify imposing greater transparency and documentation duties on platforms.

A platform should therefore be capable of demonstrating how a medication transaction occurred. When a patient alleges that an incorrect drug or dosage was delivered, the platform should be able to establish what prescription it received, what information it transmitted, whether any automated process modified that information, what medication information was displayed to the patient, and what role third-party providers played.

This does not mean that the burden of proving every element of negligence should automatically shift to the platform. Rather, it recognizes that evidence concerning the platform's internal processes is often uniquely within its control. Procedural mechanisms should prevent information asymmetry from making legitimate claims practically impossible to establish.

Patient Safety, Data Governance, and the Duty of Transparency

Medication safety in telemedicine cannot be separated from information governance. Digital healthcare depends upon the collection and processing of sensitive health information, and errors in information can affect both privacy and clinical safety.

Indonesia's Personal Data Protection Law, Law No. 27 of 2022, expressly classifies health data and information as specific personal data. The law establishes rights for data subjects and obligations for data controllers and processors concerning the processing of personal data. This framework is directly relevant to telemedicine because platforms may process medical histories, diagnoses, prescriptions, medication records, and communications between patients and healthcare professionals. The legal importance of health data in medication safety extends beyond confidentiality. Inaccurate or incomplete information can itself become a clinical risk. If a patient's allergy information is omitted from the platform's clinical interface, for example, the problem is simultaneously one of data governance and patient safety. Similarly, if a platform fails to transmit a patient's existing medication list to the physician, the resulting prescription may create an avoidable interaction.

This illustrates why digital healthcare regulation should not treat privacy and patient safety as separate silos. Data integrity is a prerequisite for safe clinical

decision-making. A platform that collects health information but fails to preserve its accuracy, completeness, or availability may create a foreseeable medication risk.

Permenkes No. 24 of 2022 concerning Medical Records provides another important element. The regulation governs medical records in the digital healthcare environment and remains in force, replacing the earlier 2008 medical-record regulation. The regulation's relevance to telemedicine lies in the need for reliable documentation of clinical interactions. Where a medication error occurs, the medical record and associated electronic records may be critical in determining what information was available to the physician, what prescription was issued, and how the prescription was subsequently processed.

The platform's duty of transparency should therefore include information about its role in the healthcare process. Patients should be able to understand whether the platform is merely facilitating communication or whether it provides additional services involving prescription processing, medication selection, pharmacy fulfillment, automated decision support, or medication information.

Transparency is not merely an ethical aspiration. It has legal significance because it allows patients to understand who is responsible for different components of care. If the platform represents itself as a comprehensive healthcare service while concealing its operational division among physicians, pharmacies, and third-party providers, patients may be unable to identify the relevant duty-holder after an injury.

The same principle applies to automated features. If a platform uses clinical decision-support tools, medication databases, automated symptom triage, or algorithmic recommendations, it should disclose the existence and material function of those tools where they can affect patient care. The World Health Organization's guidance on AI in health emphasizes transparency, accountability, human autonomy, and mechanisms for redress as central principles of responsible health technology governance (World Health Organization 2021).

Although the present article focuses on telemedicine rather than AI, the underlying governance principle is similar. Technology should not become a black box that obscures responsibility. Patients should be able to determine whether a medication decision was made directly by a physician, influenced by a digital system, modified by a platform workflow, or completed by a pharmacy. Transparency also has a direct connection to informed consent. A patient who consents to an online consultation may understand that a physician will provide medical advice, but may not understand that a platform's algorithms or databases influence the medication pathway. The legal sufficiency of consent should therefore be considered in relation to the actual structure of the service.

This does not require platforms to provide patients with extensive technical documentation. Meaningful transparency should be proportionate to the risk. A patient needs to know enough to understand how the service operates in ways that could materially affect medication safety. Technical details that have no meaningful clinical consequence need not overwhelm the patient.

The duty to maintain accurate records is equally important. A platform should preserve an auditable history of material medication transactions. If the system automatically changes prescription information, that change should be traceable. If medication information is updated, the version available at the time of the prescription should be identifiable. If a pharmacy rejects or modifies an order, the relevant communication should be recorded.

Without this level of traceability, courts may confront a fundamental evidentiary problem. The patient may have suffered harm, but the platform may possess the only evidence capable of explaining how the medication pathway operated. A liability framework that ignores this asymmetry risks making technological complexity a defense against accountability. The platform's duty should therefore include not only preventing foreseeable medication errors but also preserving sufficient evidence to investigate them. Accountability requires both prevention and reconstructability.

Toward a Functional Accountability Model for Indonesian Telemedicine

The preceding analysis supports a model in which liability is allocated according to the functional role performed by each actor rather than according to the formal identity of the contracting parties. This model can be integrated into Indonesia's existing legal framework without requiring every telemedicine platform to be treated as a hospital or physician.

The first category is professional clinical responsibility. Physicians remain responsible for the medical judgments they make within telemedicine consultations. The fact that a consultation occurs online does not eliminate professional standards. If a physician fails to obtain reasonably necessary information, misdiagnoses a condition, prescribes an inappropriate medication, or ignores clinically significant information available through the platform, professional liability may arise.

The second category is pharmaceutical responsibility. Pharmacies and pharmacists remain responsible for dispensing and medication-related professional activities within their sphere of control. If the correct prescription is transmitted but the pharmacy dispenses the wrong medication, the error should not automatically be attributed to the platform.

The third category is platform responsibility. This arises when the platform's own functions materially contribute to the medication error. Examples include inaccurate medication databases, unauthorized alteration of prescriptions, defective transmission systems, inadequate safety warnings, failure to preserve clinically relevant information, unsafe interface design, or governance failures that make foreseeable medication errors more likely.

The fourth category is third-party technological responsibility. Telemedicine platforms frequently rely on cloud providers, electronic prescribing vendors,

payment systems, pharmacy-management software, and logistics companies. Responsibility may therefore extend to external providers when a technological failure within their sphere of control materially contributes to patient harm. Contractual allocation of risk among these actors should not automatically determine the patient's substantive rights.

The fifth category is shared causation. The most realistic cases may involve multiple failures. A physician may prescribe an inappropriate dose, a platform may fail to display an interaction warning, and a pharmacy may fail to identify the discrepancy. The resulting injury may not be attributable to a single actor. The legal system should therefore permit concurrent responsibility where multiple breaches materially contribute to the harm.

The proposed functional model can be summarized through four questions, although these questions should operate as judicial reasoning rather than as a rigid statutory checklist. First, what function did the actor perform? Second, what risk was generated by that function? Third, did the actor have reasonable ability to prevent, detect, or mitigate that risk? Fourth, did the failure materially contribute to the patient's injury?

This approach is preferable to a purely contractual model. A contract may identify the platform as a service provider, but it cannot accurately describe the technical and operational realities of every transaction. Functional analysis allows the law to remain technologically neutral while responding to actual control.

The model also preserves innovation. Platforms that genuinely provide neutral infrastructure would not face automatic liability for every adverse clinical outcome. Their duties would remain proportional to their functions. At the same time, platforms that deliberately integrate themselves into clinical and pharmaceutical workflows would have incentives to implement appropriate safety controls.

The concept of proportionality is especially important. Not every platform function warrants the same level of legal responsibility. A scheduling function presents relatively low clinical risk. A medication database presents a higher risk because inaccurate information can influence treatment. An automated prescription-selection function presents an even higher risk because it can directly influence medication choice. Liability should correspond to this escalation of clinical significance. This risk-based approach also supports stronger institutional governance. Platforms should maintain procedures for medication-safety incidents, technical failures, patient complaints, and corrective action. When a recurring error is identified, the platform should investigate whether the problem arises from software, data, user-interface design, pharmacy integration, or provider behavior.

Such governance should not be treated as voluntary corporate best practice. Government Regulation No. 71 of 2019 already recognizes risk management, system governance, periodic auditing, security, and accountability as relevant obligations for electronic-system providers. The healthcare context gives these obligations greater significance because the consequences of system failure may include bodily injury rather than merely financial or informational loss.

The role of the healthcare institution must also be considered. Some telemedicine platforms operate as independent technology companies, while others are integrated with hospitals or healthcare facilities. Where the platform is operated by or under the control of a healthcare institution, institutional responsibility may be more direct. The institution may be responsible not only for physicians but also for the technological infrastructure through which care is delivered.

Law No. 17 of 2023 provides an important foundation because it recognizes patient safety and quality responsibilities within healthcare delivery. Government Regulation No. 28 of 2024 further develops the regulatory structure for health services, health facilities, pharmaceuticals, information systems, and health technology. These provisions should be interpreted in a manner that prevents healthcare organizations from separating their clinical and technological functions artificially.

The model should also preserve the patient's right to seek effective remedies. When a medication error occurs, the patient should not be forced to determine the precise technical source of the error before obtaining meaningful access to the relevant records. The platform, physician, pharmacy, and other responsible entities should maintain sufficient documentation to permit reconstruction of the transaction.

This requirement is especially important because telemedicine can create an "accountability fragmentation" problem. Each participant may point toward another actor: the physician may blame the platform, the platform may blame the pharmacy, the pharmacy may blame the electronic prescription, and the technology vendor may blame the user's input. Without a functional approach, the patient may face an accountability chain in which every actor has a partial defense but no actor provides an effective remedy. The law should resist this outcome. The complexity of service delivery should not become a basis for weakening patient protection. If multiple actors contributed to the harm, the appropriate response is to identify their respective contributions rather than to conclude that responsibility is impossible to determine.

At the same time, patient protection does not justify unlimited platform liability. A platform should not be liable for an unforeseeable adverse drug reaction merely because the patient obtained the medication through its service. Nor should a platform be responsible for a physician's independent clinical decision when the platform did not influence or alter that decision and performed its technological functions properly. The functional accountability model therefore seeks equilibrium. It recognizes that telemedicine platforms can be genuine participants in healthcare delivery without treating them as physicians. Their responsibility arises not from the mere existence of the platform but from the functions they perform and the risks those functions create.

Regulatory Implications for Indonesia

Indonesia's present framework would benefit from a more explicit regulatory articulation of platform responsibilities. The first priority should be to clarify that telemedicine platforms performing healthcare-related functions cannot rely exclusively on the legal identity of a technology intermediary when their actual operations materially affect patient care. The regulatory framework should establish a distinction between low-risk facilitation and clinically consequential platform functions. Platforms that merely provide communication infrastructure should have baseline duties concerning security, reliability, privacy, and record preservation. Platforms that manage prescriptions, medication information, pharmacy fulfillment, or automated clinical workflows should face enhanced duties proportionate to the risk of patient harm.

Such duties should include reasonable validation of medication databases, controls against unauthorized prescription alteration, auditability of prescription transmission, safety alerts for material medication risks, mechanisms for correcting erroneous information, and procedures for responding to medication-safety incidents. These requirements would not require platforms to practice medicine. They would require platforms to operate their technological systems in a manner consistent with patient safety. The regulatory framework should also address third-party integration. A platform should remain accountable for material functions it delegates to vendors. Outsourcing software or pharmacy-management services should not automatically eliminate responsibility. A platform that selects and integrates a third-party service remains in a position to assess whether the service is appropriate for the healthcare function in which it is used. This principle is consistent with the broader concept of accountability in digital governance. Outsourcing can distribute technical operations, but it does not necessarily distribute legal responsibility to the same degree. Patients interact with the integrated service, not with the contractual structure behind it.

The regulatory system should also require adequate incident documentation. A medication-safety event should trigger preservation of relevant electronic records, including prescription versions, system logs, communications, and material modifications. Such records would enable both internal investigation and legal adjudication. Patient notification should also be considered when a platform discovers that its system may have contributed to medication harm. A patient cannot make informed decisions about continued treatment if the platform knows of a material system error but does not communicate it. Transparency after an incident is therefore part of patient safety.

Finally, the regulatory framework should encourage a culture of safety rather than merely punitive compliance. Platforms should have incentives to report and correct systemic medication risks before they produce repeated patient injuries. The objective of regulation should be to make safe digital healthcare economically and organizationally rational. This approach is consistent with WHO's broader position

that digital-health interventions should be implemented within systems capable of monitoring safety, privacy, accountability, traceability, and professional standards (World Health Organization 2019). It also corresponds with the WHO's AI governance framework, which emphasizes that health technologies should protect human rights and maintain mechanisms for accountability and redress (World Health Organization 2021). The central regulatory principle should therefore be simple: the entity that meaningfully controls a healthcare risk should bear a corresponding legal duty to manage that risk. In a platform-mediated healthcare environment, this principle offers a more adaptable foundation than formal labels that may quickly become obsolete as technology evolves.

Conclusion

Telemedicine does not eliminate traditional medical liability; it reorganizes the environment in which healthcare responsibility is exercised. Medication errors in online healthcare may result from physician negligence, pharmacy failures, inaccurate medication information, defective electronic systems, unsafe platform design, inadequate patient communication, or interactions among several of these factors. Indonesia already possesses relevant legal foundations through Law No. 17 of 2023 concerning Health, Government Regulation No. 28 of 2024, Law No. 8 of 1999 concerning Consumer Protection, Government Regulation No. 71 of 2019 concerning Electronic Systems and Transactions, Law No. 27 of 2022 concerning Personal Data Protection, and Permenkes No. 24 of 2022 concerning Medical Records. These instruments collectively establish principles of patient safety, professional responsibility, electronic-system accountability, consumer protection, data governance, and healthcare quality, but they do not yet produce a sufficiently clear doctrine for determining when a telemedicine platform should be responsible for a medication error. The appropriate response is not to impose automatic liability on platforms for every adverse outcome, nor to treat platforms as legally irrelevant intermediaries. Instead, Indonesian law should adopt a functional approach under which responsibility follows the platform's actual role, degree of control, knowledge of risk, capacity to prevent harm, and contribution to the patient's injury. A platform that merely facilitates communication should not be transformed into a medical guarantor, while a platform that materially structures prescription processes, medication information, pharmacy fulfillment, or clinical workflows should bear corresponding duties of safety and governance.

A functional accountability model would provide a more coherent and equitable basis for resolving telemedicine medication disputes. Physicians should remain accountable for independent clinical negligence; pharmacies should remain responsible for dispensing failures; platforms should bear responsibility for technological and governance failures within their control; and multiple actors should be capable of bearing concurrent responsibility where their combined failures materially cause harm. The decisive question should therefore not be

whether a platform formally identifies itself as a healthcare provider, but whether it exercised meaningful control over the risk that injured the patient. This approach would also encourage better platform design, stronger auditability, clearer patient communication, and more effective incident reporting without suppressing innovation in digital healthcare. As telemedicine becomes increasingly integrated with electronic prescribing, pharmaceutical delivery, automated decision support, and health-data systems, the legal system must ensure that technological fragmentation does not become an accountability vacuum. Patient safety requires a model in which every actor that materially shapes the delivery of care carries responsibility proportionate to its capacity to prevent and mitigate harm.

References

Ammenwerth, Elske, Petra Schnell-Inderst, Christof Machan, and Uwe Siebert. 2008. "The Effect of Electronic Prescribing on Medication Errors and Adverse Drug Events: A Systematic Review." *Journal of the American Medical Informatics Association* 15 (5): 585–600. https://doi.org/10.1197/jamia.M2667.

Bashshur, Rashid L., Gary W. Shannon, Nabil Bashshur, and Dale J. Yellowlees. 2016. "The Empirical Evidence for Telemedicine Interventions in Mental Health." *Telemedicine and e-Health* 22 (2): 87–113. https://doi.org/10.1089/tmj.2015.0206.

Beauchamp, Tom L., and James F. Childress. 2019. *Principles of Biomedical Ethics*. 8th ed. New York: Oxford University Press.

Cognlianese, Cary, and David Lehr. 2019. "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era." *Georgetown Law Journal* 105: 1147–1223.

Cohen, I. Glenn, and Andrew Slottje. 2024. "Artificial Intelligence and the Law of Informed Consent." In *Research Handbook on Health, AI and the Law*. Cheltenham: Edward Elgar Publishing.

Hollander, Judd E., and Brendan G. Carr. 2020. "Virtually Perfect? Telemedicine for Covid-19." *New England Journal of Medicine* 382: 1679–1681. https://doi.org/10.1056/NEJMp2003539.

Kichloo, Asim, N. Albosta, M. Dettloff, et al. 2020. "Telemedicine, the Current COVID-19 Pandemic and the Future: A Narrative Review and Perspectives Moving Forward." *Family Medicine and Community Health* 8 (3): e000530. https://doi.org/10.1136/fmch-2020-000530.

Kruse, Clemens Scott, Priyanka Krowski, Brooke Rodriguez, Leah Tran, Jayanth Vela, and Matthew Brooks. 2017. "Telehealth and Patient Satisfaction: A Systematic Review and Narrative Analysis." *BMJ Open* 7 (8): e016242. https://doi.org/10.1136/bmjopen-2017-016242.

Mann, Rachael, et al. 2022. "Medication Safety Incidents Associated with the Remote Delivery of Primary Care: A Rapid Review." *International Journal of Pharmacy Practice* 30 (6): 495–503.

Mello, Michelle M., and Neel Guha. 2024. "Understanding Liability Risk from Using Health Care Artificial Intelligence Tools." *New England Journal of Medicine* 390 (3): 271–278. https://doi.org/10.1056/NEJMhle2308901.

Parikh, Ravi B., Michael J. Obermeyer, and others. 2021. "Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation." *Milbank Quarterly* 99 (3): 629–647.

Parimbelli, Enea, Alessandro Bottalico, Paolo Mazzola, and others. 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.

Reason, James. 2000. "Human Error: Models and Management." *BMJ* 320 (7237): 768–770. https://doi.org/10.1136/bmj.320.7237.768.

Republic of Indonesia. 1999. *Law Number 8 of 1999 concerning Consumer Protection*. Jakarta: Government of the Republic of Indonesia.

Republic of Indonesia. 2019. *Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions*. Jakarta: Government of the Republic of Indonesia.

Republic of Indonesia. 2019. *Regulation of the Minister of Health Number 20 of 2019 concerning the Implementation of Telemedicine between Healthcare Facilities*. Jakarta: Ministry of Health of the Republic of Indonesia.

Republic of Indonesia. 2022a. *Law Number 27 of 2022 concerning Personal Data Protection*. Jakarta: Government of the Republic of Indonesia.

Republic of Indonesia. 2022b. *Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records*. Jakarta: Ministry of Health of the Republic of Indonesia.

Republic of Indonesia. 2023. *Law Number 17 of 2023 concerning Health*. Jakarta: Government of the Republic of Indonesia.

Republic of Indonesia. 2024. *Government Regulation Number 28 of 2024 concerning the Implementing Regulation of Law Number 17 of 2023 concerning Health*. Jakarta: Government of the Republic of Indonesia.

Roumeliotis, Nadia, Jonathan Sniderman, Thomasin Adams-Webber, et al. 2019. "Effect of Electronic Prescribing Strategies on Medication Error and Harm in Hospital: A Systematic Review and Meta-Analysis." *Journal of General Internal Medicine* 34 (10): 2210–2223. https://doi.org/10.1007/s11606-019-05236-8.

Smith, Helen, and Kit Fotheringham. 2020. "Artificial Intelligence in Clinical Decision-Making: Rethinking Liability." *Medical Law Review* 28 (4): 636–657.

Tobia, Kevin, Daniel M. H. Nielsen, and others. 2021. "When Does Physician Use of AI Increase Liability?" *Journal of Nuclear Medicine* 62 (1): 17–21.

Wootton, Richard. 2012. "Twenty Years of Telemedicine in Chronic Disease Management—An Evidence Synthesis." *Journal of Telemedicine and Telecare* 18 (4): 211–220. https://doi.org/10.1258/jtt.2012.120219.

World Health Organization. 2017. *Medication Without Harm: WHO Global Patient Safety Challenge on Medication Safety*. Geneva: World Health Organization.

World Health Organization. 2019. *WHO Guideline: Recommendations on Digital Interventions for Health System Strengthening*. Geneva: World Health Organization.

World Health Organization. 2021. *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*. Geneva: World Health Organization.

***

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