International Journal of Innovative Research and Scientific Studies, 8(3) 2025, pages: 3581-3590

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Legal framework chamber of governance digital health innovation: Insights from implementation of health technology transformation in Indonesia

Rico Mardiansyah[1*], Edmon Makarim[2], Sulistyowati[3]

[1,2,3]*University of Indonesia, Depok, Indonesia.*

Corresponding author: Rico Mardiansyah (*Email: rico.mardiansyah@gmail.com*)

Abstract

In Indonesia, the rapid advancement of digital health technology has significantly impacted the healthcare sector, driving innovation while presenting numerous regulatory challenges. This study aims to explore the legal framework governing digital health innovation in Indonesia, with a focus on telemedicine systems and personal data protection. Through a qualitative socio-legal approach, the research examines the regulatory challenges and governance structures in place to address the issues arising from technological disruptions in healthcare. The study utilizes primary data from interviews with key stakeholders, including government officials and health tech entrepreneurs, alongside secondary data from legal texts and policy documents. Findings indicate the necessity of an agile governance model that allows for the rapid adaptation of policies to support technological advancements while safeguarding public interests. The study concludes that a flexible and multi-stakeholder approach to policy development is essential for fostering innovation while ensuring patient safety and data security. By adopting regulatory sandboxes and integrating experimental governance models, Indonesia can effectively navigate the challenges posed by digital health innovations and achieve a balanced and sustainable health tech ecosystem.

Keywords: Agile governance, digital health, Indonesia, legal framework, technological innovation.

DOI: 10.53894/ijirss.v8i3.7318
Funding: This study received no specific financial support.
History: Received: 3 April 2025 / **Revised:** 7 May 2025 / **Accepted:** 9 May 2025 / **Published:** 23 May 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The era of globalization and rapid technological change has driven the massive development of digital health service innovations. These innovations affect daily behavior and interactions, creating numerous opportunities for new business forms and innovations that disrupt conventional health service businesses. The development of digital health services requires policymakers to find ways to balance innovation and regulation while remaining flexible in the face of rapid technological changes. Generally, policymaking processes lag behind the speed of technological innovation, where the use of information

technology in health services raises various challenges related to legal, ethical, and governance issues. Conventional legal concepts become increasingly obsolete, necessitating the development of alternative perspectives on the regulatory challenges created by the new innovation-driven global economy [1]. The challenge in regulating innovation involves creating regulatory concepts that are fit for rapid technological advancements and disruptions [2].

Information technology advances, part of the digital economy's development, are defined as the combination of mobile technology, internet access, the shift toward cloud storage, and data analysis that alters economic dynamics [3]. The current rapid advancement of information technology is categorized as the fourth industrial revolution, where industry players develop their business lines by leveraging information technology. This linear development of information technology with the industrial sector positively impacts the country, including economic growth [4].

The digital economy, utilizing information technology advancements as part of the fourth industrial revolution, is characterized by unprecedented technological advancements that alter how individuals and groups across society work and interact daily. This requires new principles, protocols, rules, and policies to positively and inclusively impact technology utilization while minimizing or eliminating negative consequences [5]. Generally, policy-making processes lag behind the speed of technological innovation, hence, society expects the private sector and non-governmental entities to take on new responsibilities and develop new approaches to support diversification and agility in achieving good governance in utilizing technological innovations. Therefore, this fourth industrial revolution necessitates the transformation of governmental structures and the development of policy-making models within an agile governance concept [5]. Agile governance is defined as adaptive, human-centered, inclusive, and sustainable policy-making, recognizing that policy development is no longer limited to the government but is a multi-stakeholder effort to navigate changes quickly and proactively embrace and learn from them [5].

In a constant or non-adaptive regulatory condition towards innovation, digital innovation becomes a "minefield" for innovators and businesses, where innovators risk sanctions from norms developed before digital innovation [6]. Policymakers must create favorable conditions for the safe and beneficial development of technology or innovation for regulators, business innovators, and consumers. Thus, new regulatory instruments are needed for the utilization of digital technology that can respond to public and private interests.

Unprecedented global transformation has led regulators to balance traditional regulatory objectives, economic stability, and consumer or public protection to foster innovation and growth. The emergence of digital innovation creates new opportunities and risks. This fact influences government efforts to develop regulations suitable for digital reality conditions, requiring policymakers to develop new approaches to digital technology regulation [7].

The previous research has been done by Glanowski [6]. This study discusses the legal implications of telemedicine and the regulatory challenges in the digital health market, particularly in European contexts, which may offer comparative insights for Indonesia’s regulatory framework in digital health innovation.

Furthermore, Zetzsche et al. [7]. "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation." Fordham Journal of Corporate and Financial Law, Vol. XXIII. This paper explores the use of regulatory sandboxes as a method to foster innovation while managing risks, which is highly relevant to the implementation of agile governance in digital health innovation in Indonesia.

This study aims to analyze the legal framework of digital health innovation in Indonesia, focusing on regulatory challenges arising from the rapid development of health technology. This research also aims to identify the policies and legal instruments needed to support the implementation of health technology innovations in Indonesia, especially related to telemedicine systems and personal data protection. In addition, this study explores agile governance models in the context of digital health policies to ensure that these policies can adapt to rapid technological changes. This study also aims to assess the social and economic impact of the application of digital health technology in Indonesia, taking into account the benefits and risks posed to the public and the health sector.

The benefit of this research is to provide insight for policymakers on the importance of flexible and adaptive policy formulation to support the development of digital health technology, as well as to address the regulatory challenges faced by Indonesia. This research is also expected to help design more effective policies and regulations related to the use of digital technology in the health sector, especially to create a safe testing ground for innovations through instruments such as regulatory sandboxes. In addition, this research is useful for improving the understanding of digital governance in the health sector, which enables stakeholders to better manage potential risks related to data privacy and cybersecurity in digital healthcare.

2. Methodology

This study adopts a qualitative socio-legal approach to examine the legal framework and governance structure for digital health innovation in Indonesia. Socio-legal research does not merely view law as a system of written rules but rather as a dynamic institution that interacts with social structures, actors, and cultural values [8]. Within this framework, law is explored both as a normative system and as a set of practices embedded in broader institutional contexts that include regulators, healthcare professionals, health tech innovators, and users.

The qualitative design is appropriate to address the core research questions concerning how digital health innovation is developed and regulated, how accountability and responsibility are constructed, and what socio-economic impacts emerge from the digital transformation of healthcare. This study seeks to explore the legal-institutional equilibrium between regulation and innovation by analyzing how experimental governance instruments, particularly regulatory sandboxes, are implemented and adapted in practice [9].

Primary data were collected through in-depth, semi-structured interviews with key stakeholders, including officials from the Ministry of Health, the Ministry of Communication and Informatics, and the National Cyber and Crypto Agency (BSSN). Other informants included representatives from startups such as Halodoc, Lifepack, and Zicare. These interviews provided a holistic, grounded understanding of both public and private sector roles in the digital health ecosystem.

Additionally, non-participant observation was conducted on-site during digital service implementation, especially in telemedicine and regulatory sandbox trial environments, to capture day-to-day operational realities and governance responses. Observational data were used to triangulate interview findings and to contextualize field narratives.

Secondary data were compiled through doctrinal legal research. These included statutory documents such as Law No. 17/2023 on Health, Law No. 27/2022 on Personal Data Protection, Government Regulation No. 28/2024, and Ministerial Decree No. HK.01.07/MENKES/1280/2023 regarding the regulatory sandbox for health innovation. The analysis was further supported by international policy documents and academic literature from institutions such as the WHO and OECD [10, 11].

Thematic analysis was employed to process and interpret the data. Following Braun and Clarke [12] six-phase model familiarization, coding, theme development, theme review, theme definition, and writing the study applied qualitative coding to transcripts, observational field notes, and legal texts. Triangulation across sources and methods ensured analytic validity, while theoretical interpretation was anchored in the concepts of responsive regulation, digital innovation law, and adaptive governance [13].

3. Results and Discussion

3.1. Legal Framework Chamber of Governance Digital Health Innovation

Public and business interests in health technology development can be viewed from various perspectives. One literature categorizes dimensions of public interest and business interest in technology development as follows [14].

1. Individual Impact Dimension: Healthcare service providers or human resources in healthcare have a negative perception of health technology development due to doubts about its effectiveness, concerns about safety, privacy abuse risks, and increased workload [15].
2. Technical Dimension: This dimension concerns the technical relationship between public and business interests in technology development, such as inadequate devices, poor internet connection, inadequate infrastructure, and lack of individual understanding of the technology [16].
3. Organizational Dimension: This dimension involves policy stakeholders, service providers, and service users. Integration among these elements is needed, and it is crucial to listen to and aggregate needs. Some countries have even established independent organizations to regulate health technology [17].
4. Financial Dimension: For years, public behavior has received much attention as a possible explanation for health disparities. Health-related behavior is based on the choices available to individuals, which vary according to their social position [18].

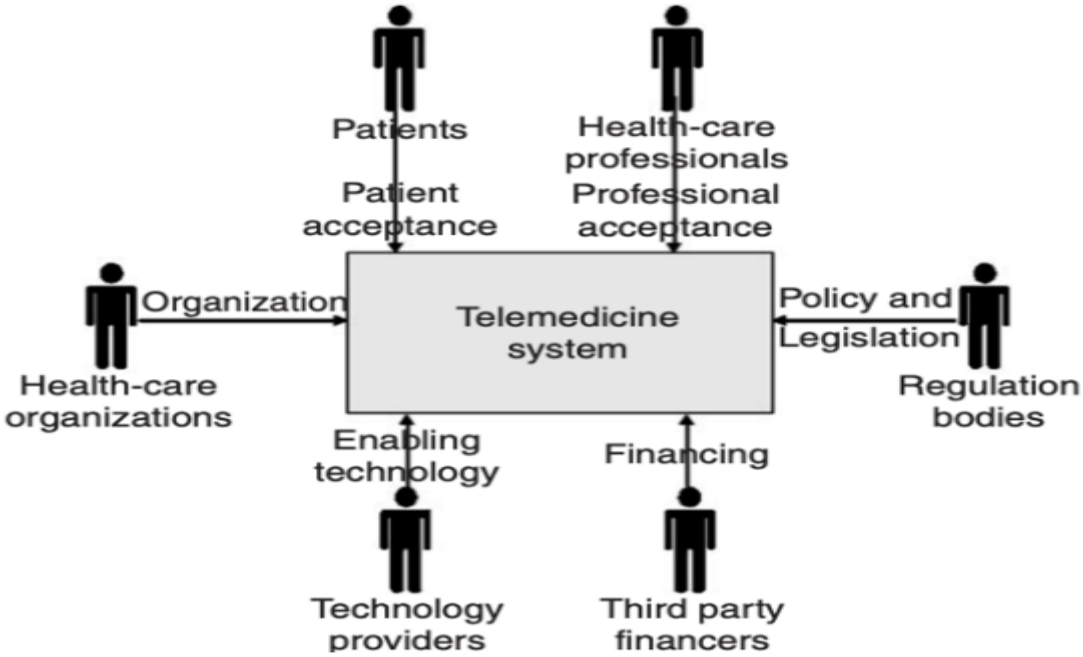

Figure 1.
Dimensions of Public Interest in the Telemedicine System Process.

Developing telemedicine implementation is a multidisciplinary activity. It is essential to gather domain-specific knowledge regarding various determinants by involving domain-specific stakeholders. However, the main challenge of implementing telemedicine is not only overcoming specific domain problems but also integrating related domains through organizational collaboration (business, government, and healthcare services) [19].

Furthermore, utilizing information technology currently serves as a support for health information system transformation. According to Law No. 17 of 2003 on Health, the health information system integrates various stages of processing, reporting, and using information necessary to enhance the effectiveness and efficiency of health services and direct actions or decisions that support health development (Indonesia, Law No. 17 of 2003). The government is responsible for ensuring the sustainability and benefits of Health Technology innovation through limited-scale testing of Health Technology, cross-stakeholder collaboration approaches to encourage innovation development, product/service utilization expansion, and innovation-based policy formulation.

The implementation of telemedicine in Indonesia is a complex and inherently multidisciplinary endeavor. It demands not only technological innovation but also synchronized efforts in policymaking, legal adaptation, health system transformation, and stakeholder engagement. Telemedicine serves as a strategic solution to address healthcare disparities, particularly the unequal distribution of medical personnel and infrastructure between urban centers and remote regions. Successful implementation requires the integration of domain-specific knowledge from different sectors health, digital infrastructure, and governance through structured organizational collaboration involving the state, private sector, and civil society.

Information and communication technology (ICT) plays a foundational role in supporting the transformation of health information systems. According to Article 205 of Indonesia's Health Law No. 17 of 2023, the health information system is expected to integrate data processing, reporting, and utilization across various levels of healthcare services. The goal is to improve the effectiveness and efficiency of service delivery while enabling evidence-based decision-making to support public health objectives [20]. In line with this mandate, the government is tasked with ensuring the sustainability of health innovation by promoting pilot projects, cross-sector collaborations, scalable product deployments, and regulatory frameworks grounded in agile innovation principles.

To effectively foster digital innovation while maintaining public trust and regulatory coherence, governments and institutions have adopted experimental governance models that allow for agile, iterative testing of new technologies and business models. Among the most prominent mechanisms are innovation laboratories, which serve as controlled environments where stakeholders can explore, assess, and validate technological solutions before full-scale implementation. These labs are designed not only to accelerate innovation but also to manage the legal, technical, and societal uncertainties that often accompany emerging technologies.

In the context of health technology innovation, where regulatory lag, market readiness, and ethical implications are critical innovation labs function as a bridge between experimentation and policy development. They provide a structured framework for testing, feedback, and adaptive governance. The following section outlines three key types of innovation laboratories commonly adopted by regulatory institutions: innovation labs (focused on exploration and experimentation), industrial labs (focused on practical application and scaling), and regulatory labs (focused on regulatory alignment and policy development). Each plays a unique role in building an innovation ecosystem that is both dynamic and accountable.

1. Innovation Development (innovation lab): Innovation labs function as spaces for exploring innovative technologies and business models and detecting opportunities and risks [21]. Bank Indonesia uses innovation labs to test new or limited-use technology development in payment systems. In Europe, innovation labs help law enforcement investigate and analyze the benefits, threats, and opportunities of new technologies [22].
2. Product and Service Utilization Expansion (industrial lab): Industrial labs synergize digital innovations with concrete needs in the real sector [21]. Bank Indonesia uses industrial labs to test widely-used payment system technology innovations and encourage broader use [21].
3. Innovation-Based Policy Formulation (regulatory lab): Regulatory labs test the conformity of innovative technologies and business models with existing regulations [21]. Bank Indonesia continues to use regulatory sandboxes to test industry-used payment system innovations and encourage broader use. Health technology innovations lack clear standards or guidelines. The IMF developed a model/framework for policymakers to narrow down the health sandbox focus area [23].

Figure 2.
Health RegLab Design Elements.

The advancement of digital health governance in Indonesia demands not only the establishment of comprehensive regulation but also the assurance that such frameworks remain resilient, adaptive, and sustainable. According to Jessy, a representative of Zicare, effective legal reform in the health sector must account for the long-term sustainability of digital systems rather than merely responding to present technological developments. She emphasized that regulatory initiatives should be built to evolve alongside innovation, allowing emerging technologies to flourish without compromising patient safety, data protection, or digital system integrity. In her view, regulatory flexibility must be supported by a structured governance framework capable of absorbing continuous technological change while upholding ethical and legal safeguards that protect the public interest [24].

Furthermore, Jessy underscored the importance of establishing routine policy evaluation mechanisms. Such mechanisms are essential to identify gaps in the implementation of digital health systems, allowing policymakers to calibrate strategies and maintain alignment with the ever-evolving demands of health service delivery. She argued that with firm cross-sectoral commitment and stricter standards for interoperability, data transparency, and patient privacy, Indonesia's digital health system could become a modern, trusted, and inclusive platform for healthcare. If applied correctly, digitalization will not only improve service efficiency but also increase public trust in domestic health services, thereby reducing national dependence on international healthcare providers.

This perspective is complemented by Ricky, a senior official from the National Cyber and Crypto Agency (BSSN), who acknowledged that Indonesia already possesses a relatively detailed set of digital health regulations. However, he stressed that implementation challenges persist, particularly in relation to technical capacity, user awareness, and institutional coordination. According to Ricky, existing laws provide a critical baseline, but policy execution often falters due to fragmentation across agencies and insufficient integration with real-time operational needs. He called for greater synergy among stakeholders and emphasized that cybersecurity practices must be continuously improved and strategically evaluated to ensure regulatory instruments achieve their intended outcomes.

The necessity for evidence-based regulation is further underscored by the rapid uptake of health information technologies (HITs) during the pandemic. Health providers were required to adapt immediately to tools such as electronic medical records (EMRs), telemedicine platforms, robotics, and biomedical technologies. This shift revealed the importance of not only investing in digital infrastructure but also of building regulatory frameworks that evolve in tandem with innovation. The IMF developed a model/framework for policymakers to narrow down the health sandbox focus area [25]. According to this model, any regulatory structure supporting digital innovation particularly in health must ensure the following components:

1. Boundaries and Safeguards: Trial limitations, target user criteria, and structured exit strategies.
2. Customer Protection Mechanisms: Transparency obligations, testing disclosures, and compensation processes.
3. Risk Management Systems: Privacy protocols, cybersecurity readiness, and institutional technical competence.

These principles should guide Indonesia's approach to digital health governance. By building frameworks grounded in regulatory agility, public protection, and multi-stakeholder accountability, Indonesia can not only keep pace with technological development but also position itself as a leader in responsible health innovation in the region.

Table 1.
Evolution of Healthcare Sector Focus: Comparison between Medical Products, Medical Platforms, and Smart Medical Solutions in Three Decades.

Decade Before	Current Decade	Next Decade
Focus on Medical Products	Focus on Medical Platforms	Focus on Medical Solutions
Medical Products (hardware, consumer goods)	Big Data (wearables, health analysis)	Robotics, AI, augmented reality
Differentiation focuses on medical products. Medical products are evidence-based.	Health services differentiation considers stakeholders. Services are outcome-based.	Differentiation focuses on intelligent solutions based on evidence. Intelligent solutions are prevention and care-based.

Adapting health information technology requires reorganizing infrastructure, policy planning, and priority achievement. The adaptation of health information technology aims to increase patient triage capacity, infection control, medication management, remote patient communication, and other goals, posing challenges for the adaptation of health information technology [26].

Information technology underpins the government's response to coordinating societal needs with clinical actions, requiring quick infrastructure, policy, and priority adjustments. Timely communication between patients and health service providers is crucial. Increased information technology access can enhance medical record exchange capabilities with additional service providers for patients transferred to other facilities, matching patients with community service providers [27]. Considerations include simplifying orientation, reducing training time, increasing security, providing information to healthcare providers about phishing and other attacks, and providing resources for reporting them. Telemedicine and telehealth activities use technology for health services [28].

3.2. Accountability and Responsibility in Digital Health Innovation

Ricky Aji from the National Cyber and Crypto Agency (BSSN) explained that Indonesia's cybersecurity regulations are currently based on two foundational legal instruments: the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law). The ITE Law governs electronic interactions and digital transactions, while the PDP Law is designed to safeguard individual privacy in digital environments. However, according to Ricky, both laws still

exhibit structural weaknesses, particularly in terms of their broad and ambiguous regulatory scope, as well as the limited effectiveness of enforcement in practice.

Ricky noted that both laws have not fully adapted to the increasingly sophisticated landscape of cyber threats. These instruments are not yet capable of adequately addressing complex, cross-border, and sector-transcending cybersecurity challenges. He emphasized that the current regulatory scope lacks depth in areas such as real-time incident response, international collaboration mechanisms, and technical enforcement for digital health systems.

One of the most pressing issues identified is the low rate of cyber incident reporting among electronic system providers. Organizations are often reluctant to report breaches due to concerns over reputational damage, public trust erosion, or legal liability. As a result, many cybersecurity incidents remain undisclosed or underreported, impeding national-level efforts to analyze threat patterns and deploy timely countermeasures. Ricky argued that this reflects a deeper cultural issue: a lack of transparency and accountability within digital service providers in both the public and private sectors.

To address this, Ricky proposed a set of strategic solutions.

1. Enhancing cybersecurity literacy among system administrators and business leaders through national education programs.
2. Creating policy protections that incentivize honest reporting of breaches, including legal immunity or safe harbor clauses.
3. Establishing integrated reporting systems that are accessible, anonymized, and responsive to diverse cybersecurity scenarios.

Ricky also highlighted the limited technical capacity and resource constraints faced by small and medium-sized enterprises (SMEs), which struggle to comply with complex cybersecurity standards. These challenges are often compounded by inadequate interagency coordination, resulting in regulatory gaps across institutions. To overcome this, he called for a holistic and collaborative model of cybersecurity governance that emphasizes interoperability, knowledge-sharing, and accountability mechanisms.

This structured approach reflects global trends that center on accountability as a pillar of digital health governance. Responsible digital innovation requires open systems where stakeholders can identify, address, and resolve risks collectively. It also demands compliance with evolving ethical standards and user protection frameworks. Digital innovation outcomes particularly in healthcare must ensure system reliability, transparent communication, and stakeholder responsiveness.[29].

From a cybersecurity standpoint, electronic system operators must ensure data confidentiality, integrity, and availability, commonly referred to as the CIA triad. As Feigenbaum defines it, accountability implies responsibility for implementing and enforcing digital policies, with corresponding legal liabilities when those policies are breached. Gajanayake further argues that system accountability includes the obligation to justify operational decisions and guarantee authorized data access only [30]. These standards align with ISO/IEC 27002:2013, which formalizes global best practices in health information security, particularly as it applies to patient data protection and digital trust.

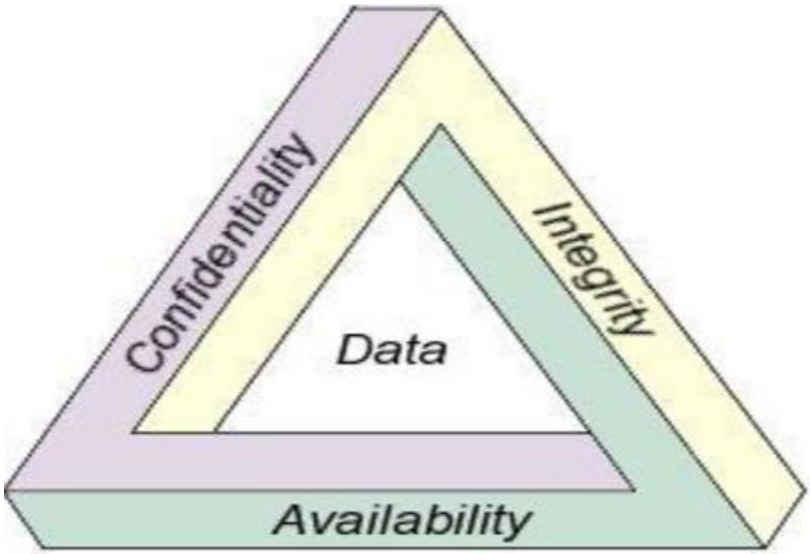

Figure 3.
Three aspects of information security (CIA) by Pfleeger.

Whitman and Mattord further stated that information security is the protection of information and its critical elements, including the systems and hardware used to store and send information. Whitman and Mattord added one aspect of accuracy, authenticity, usefulness, and ownership to the list of information characteristics that need to be protected. There are several experts who also criticize the CIA because it considers its orientation and technical focus to be too narrow.

Aside from that, accountability also requires access control, which is one of the features that plays an important role in ensuring the security of the system used. Access management is divided into three phases: the first two phases relate to subject interactions, and the third phase relates to objects (identification, authentication, and authorization). Electronic system users who want access need to first carry out a user identity identification process or biometric interaction.

The purpose of user identification is to ensure user accountability so that at the next stage, it can be guaranteed that only authorized users can disclose information they know or have about themselves. The next phase is that authorization is carried out, and the list of controlled objects is determined along with the permissions that have been granted to the user [31]. In the US, in 1992, Role-Based Access Control (RBAC) was formalized and published in 2000 to address the need for authorization control over objects and added maintenance/administration features to group users who have the same permissions/needs. The RBAC model separates core, hierarchical, static task relationships and dynamic task relationship separation to address a single organization's security policy strategy. Role-Based Access Control (RBAC) can be illustrated with the following image:

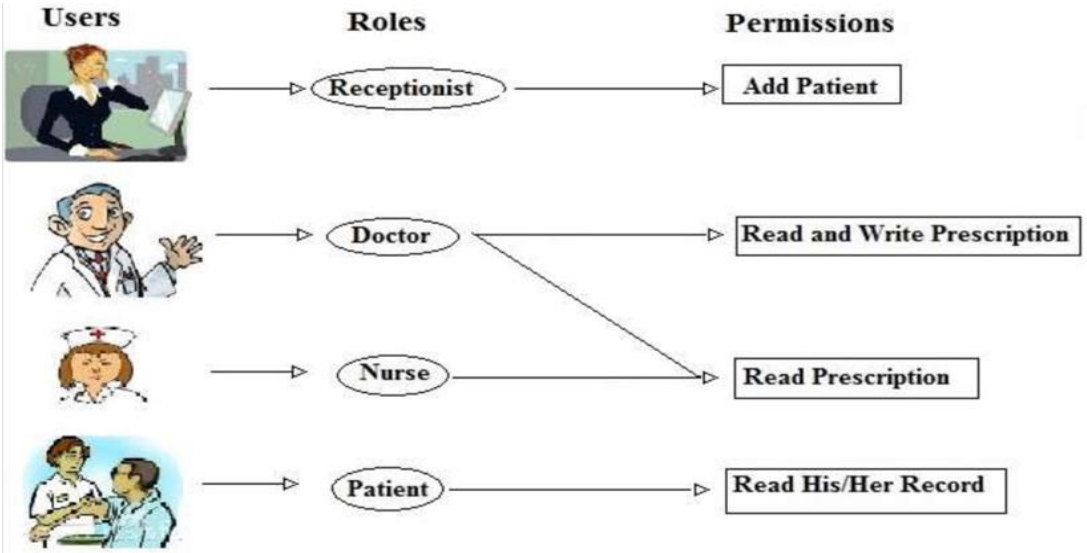

Figure 4.
Role-Based Access Control (RBAC).

The successful implementation of digital health systems requires not only technological preparedness but also strong human factor alignment particularly from frontline medical professionals. One critical barrier, as observed by Jessy, a digital transformation officer from Zicare, is the resistance among healthcare workers, especially doctors and nurses, who have been accustomed to manual record-keeping for decades. Many medical staff perceive digital systems as burdensome and unnecessary disruptions to well-established routines. This sentiment stems from discomfort with new technologies, reluctance to alter long-standing habits, and fear that digitization may interfere with their clinical workflow.

Beyond habit, this resistance is also rooted in psychological apprehensions. Jessy explained that many healthcare workers fear the uncertainty that comes with adopting new systems such as Electronic Medical Records (EMRs). The shift requires them to adapt to new methods of handling patient data, including how they input diagnoses, access historical records, and document treatments. For those with limited digital literacy, EMRs may appear more confusing than helpful. The transition from paper-based to digital systems is not only a technical challenge but is also perceived as an added workload, particularly for practitioners already stretched thin with clinical duties.

Furthermore, some physicians express concern that digital systems reduce the efficiency of care delivery. Unlike manual note-taking, which they consider quicker and more intuitive, entering structured data into a digital system is seen as time-consuming. This leads to fears that doctors will spend more time looking at screens than interacting with patients, contradicting the primary goals of digitalization namely, improving efficiency, patient-centeredness, and quality of care.

Importantly, the resistance is not merely technical it is also cultural and institutional, particularly about transparency and accountability. In manual systems, entries are flexible and relatively difficult to audit externally. But in digital systems, every modification to a patient's medical record is logged and traceable, making all medical actions more visible and auditable. While this enhances accountability, some clinicians perceive it as a threat to their professional autonomy, fearing that any deviation or error could be easily detected and questioned.

The issue of digital access and authorization is also crucial. Digital systems in healthcare increasingly rely on Role-Based Access Control (RBAC) frameworks, which determine who can access what information based on predefined roles and responsibilities. As described in the RBAC model, hospital workers are assigned system roles that mirror their actual duties ensuring that sensitive information is only available to authorized individuals [32]. This model defines hierarchical role mapping, user-task separation, and system-object interactions. When implemented properly, RBAC is fundamental to maintaining patient data security, preventing unauthorized access, and promoting institutional accountability.

In implementing electronic systems, there are IT Governance principles/information and communication technology governance in which there are elements of legal compliance in the implementation of corporate governance (leadership, organizational structure, and processes that ensure organizational performance). In order to ensure compliance with the implementation of electronic system governance with existing regulations/standards, an audit should be carried out. Audits are also conducted as an effort to manage legal risks regarding potential legal problems that may arise as a result of negligence or loss.

3.3. Digital Health Innovation Benefits

The increasing complexity of Indonesia's digital health ecosystem demands a more integrative, dynamic, and responsive regulatory framework. According to Luat Sihombing, effective regulation must strike a balance between public protection and the need for continuous innovation in health technology. A well-adapted regulatory system not only provides legal certainty for service providers but also ensures that digital health users are shielded from both legal and technological risks.

Luat identified several pressing challenges. First, fragmented coordination across ministries, especially between the Ministry of Health and the Ministry of Communication and Informatics, has led to regulatory blind spots. He emphasized the need for an inter-ministerial synergy to create a streamlined and enforceable oversight framework. Second, he advocated for strengthening the regulatory sandbox not only as a testing space for digital innovations but also as a platform for legal and technological literacy providing a controlled environment to trial new models before broad deployment. The IMF developed a model/framework for policymakers to narrow down the health sandbox focus area [23].

Third, Luat argued that the current Electronic System Operator (PSE) registration mechanisms in health care require reform. Tighter verification standards are necessary to ensure that only service providers who meet security and legal compliance thresholds can operate. Without this, the risk of data breaches and substandard health practices will increase.

Fourth, he highlighted the importance of transparent and responsive complaint mechanisms, where public input and whistleblower reporting play a crucial role. Integrating AI and big data into this system would enhance pattern detection and regulatory responsiveness. Fifth, in the realm of personal data protection, Luat called for an urgent issuance of implementing regulations under the Personal Data Protection Law, aligned with international data security standards such as ISO 27001. He also proposed periodic external audits to ensure sustainable compliance.

From a socio-legal perspective, these recommendations align with the idea that law should not merely regulate but also facilitate responsible innovation. Evidence-based and risk-based regulation models are essential for ensuring that technological progress advances in step with public interest and legal legitimacy.

In the domain of telemedicine, the role of law is pivotal in guiding both the trajectory and sustainability of health innovation. According to Irwan [33], the future of telemedicine depends heavily on a regulatory ecosystem that achieves an optimal balance between innovation, public demand, and legal protection.

He warned that over-regulation could stifle the potential of telemedicine to solve long-standing health access inequalities. Conversely, overly permissive regimes may jeopardize patient safety and clinical quality. The solution, he argues, lies in a risk-based regulatory approach, one that focuses on issues directly related to patient risk, clinical standards, and personal data security. Such regulation can promote innovation while offering clear legal safeguards to users and providers alike.

Irwan further stressed the importance of inclusive multi-stakeholder collaboration. Regulators, professional associations, and digital health entrepreneurs must jointly design risk-based policies that reflect the practical realities of care delivery. This approach helps ensure that policies are not top-down but also rooted in the lived experiences of practitioners and users. With this model, telemedicine regulation becomes both a driver of innovation and a guarantor of patient protection.

In a parallel interview, Aji [34] of BSSN emphasized the need for synchronizing adaptive regulation with high public cybersecurity literacy. He defined adaptive regulation as flexible laws capable of responding to the evolving nature of cyber threats. Such regulation must facilitate innovation while protecting personal data and critical systems from ever-changing digital risks.

However, Aji [34] noted that even the most well-crafted regulation will fail in practice if citizen awareness is low. He advocated for sustained, multi-sectoral public education campaigns that build digital hygiene, explain cybersecurity threats, and foster proactive digital practices. In health, specifically, where data sensitivity is high, flexible legal instruments must be accompanied by a robust security culture.

Global partnerships and cloud-based infrastructure are helping bridge these gaps. Recent statistics show that over 80% of people in developing countries have mobile phones, and nearly half the global population uses the internet [35]. These figures support broader investments in data-driven innovation, particularly in areas such as disease prediction, preventive care, and population health management [36].

Indonesia’s path toward a robust digital health ecosystem lies in its ability to harmonize law, innovation, and social inclusion. As this elaboration shows, insights from Luat Sihombing, Dr. Irwan, and Ricky Aji underscore the importance of building regulations that are adaptive, risk-based, and rooted in practical realities. Such regulations should not only protect but also empower by offering safe spaces for innovation, ensuring digital equity, and fostering a future-ready health system.

4. Conclusions

Rapid technological advancements and globalization have significantly driven digital health innovation in Indonesia. These changes affect daily behavior and interactions, create new business opportunities, and disrupt conventional health service models. Policymakers face the challenge of balancing innovation and regulation and must remain flexible in the face of rapid technological changes. This research explores the legal framework for digital health innovation governance in Indonesia, analyzing the regulatory challenges and perspectives needed to navigate the innovation-driven global economy. The study highlights the importance of an agile governance model to support technological advancements in health services.

Digital technology application in health services raises various legal, ethical, and governance challenges. A robust regulatory framework is needed to accommodate technological advancements like AI-based diagnostics, telemedicine, and patient data protection. This study emphasizes the need for a permissive regulatory regime to encourage innovation. Policymakers must create favorable conditions for safe and beneficial technology development, involving innovation labs for exploring new technologies, industrial labs for integrating digital innovations with real sector needs, and regulatory labs for testing innovative business models' compliance with existing regulations or providing policy recommendations based on

technological advancements. Digital health innovation also requires transforming bureaucracy into agile organizations capable of responding quickly and flexibly to changes. Agility is crucial for maintaining organizational effectiveness and efficiency in the face of rapid technological advancements. The social and economic benefits of digital health innovation are significant, contributing to improved healthcare access, job creation, and greater global connectivity.

A future-proof regulatory framework must support sustainable digital health technology development and integration while protecting public and private sector interests. This comprehensive regulatory approach will enable Indonesia to leverage the full potential of digital health innovation, ultimately improving health outcomes and economic growth.

References

[1] M. Corrales Compagnucci, T. Kono, and S. Teramoto, *Legal aspects of decentralized and platform-driven economies. In M. Corrales Compagnucci, N. Forgó, T. Kono, S. Teramoto, & E. P. M. Vermeulen (Eds.), Legal Tech and the New Sharing Economy*. Springer. https://doi.org/10.1007/978-981-15-1350-3_1, 2020.

[2] R. Brownsword, E. Scotford, and K. Yeung, *The Oxford handbook of law, regulation and technology*. Oxford, UK: Oxford University Press, 2017.

[3] B. Van Ark, "The productivity paradox of the new digital economy," *International Productivity Monitor*, vol. 31, pp. 3-18, 2016. https://doi.org/10.1787/ipm-31-5jrsqk7q3v8v

[4] M. o. C. a. I. Center for Research and Development of Informatics Applications and Public Information and Communication Agency for Research and Development of Human Resources, *The impact of information technology on economic growth in Indonesia*. Jakarta, Indonesia: Ministry of Communication and Information Technology of the Republic of Indonesia, 2018.

[5] World Economic Forum, *The future of jobs report 2018*. Geneva, Switzerland: World Economic Forum, 2018.

[6] G. Glanowski, "Legal status of telemedicine in the internal market," *European Journal of Health Law*, vol. 23, no. 3, pp. 231-247, 2016. https://doi.org/10.1163/15718093-12341414

[7] D. A. Zetzsche, R. P. Buckley, J. N. Barberis, and D. W. Arner, "Regulating a revolution: From regulatory sandboxes to smart regulation," *Fordham Journal of Corporate & Financial Law*, vol. 23, p. 31, 2017. https://doi.org/10.2139/ssrn.3018534

[8] S. Halliday and P. Schmidt, *The law as a social institution*. Oxford: Oxford University Press, 2009.

[9] J. Black and R. Baldwin, "Really responsive risk-based regulation," *Law & Policy*, vol. 32, no. 2, pp. 181-213, 2010. https://doi.org/10.1111/j.1467-9930.2010.00318.x

[10] Organisation for Economic Co-operation and Development (OECD), *The role of innovation in health policy and economic development*. Paris, France: OECD Publishing, 2020.

[11] World Health Organization (WHO), *Global health and regulatory frameworks for innovation in healthcare*. Geneva, Switzerland: World Health Organization, 2021.

[12] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006. https://doi.org/10.1191/1478088706qp063oa

[13] N. Purtova, "Do property rights in personal data make sense after the big data turn: Individual control and transparency," *Journal of Law and Economic Regulation*, vol. 10, no. 2, pp. 64-78, 2017. https://doi.org/10.2139/ssrn.3070228

[14] T. H. F. Broens, R. M. H. A. Huis in't Veld, M. M. R. Vollenbroek-Hutten, H. J. Hermens, A. T. van Halteren, and L. J. M. Nieuwenhuis, "Determinants of successful telemedicine implementations: A literature study," *Journal of Telemedicine and Telecare*, vol. 13, no. 6, pp. 303-9, 2007. https://doi.org/10.1258/135763307781644951

[15] R. Wootton, *Telehealth in the developing world*. Ottawa, Canada: IDRC, 2009.

[16] P. A. H. O. P. World Health Organization (WHO), *eHealth in the Americas: Building resilience to a changing health landscape*. Geneva, Switzerland: World Health Organization. https://doi.org/10.1590/2316-4178/jdcl.2016.0301, 2016.

[17] American Telemedicine Association, *Regulating health technology: Challenges and opportunities in the digital age*. Washington, D.C: American Telemedicine Association, 2022.

[18] P. Drahos, *Regulatory globalisation. In Regulatory Theory*. Oxford, UK: Oxford University Press, 2017.

[19] M. Scheffler and E. Hirt, "Wearable devices for telemedicine applications," *Journal of Telemedicine and Telecare*, vol. 11, no. 1_suppl, pp. 11-14, 2005. https://doi.org/10.1258/1357633054461994

[20] Indonesia, *Regulatory mandate for health innovation sustainability: Promoting pilot projects and cross-sector collaborations*. Jakarta, Indonesia: Ministry of Health of the Republic of Indonesia, 2023.

[21] Bank Indonesia, *Strategic roadmap for digital innovation in the banking sector*. Jakarta, Indonesia: Bank Indonesia, 2019.

[22] European Union Agency for Law Enforcement Cooperation, *Annual report 2023*. Brussels, Belgium: European Union, 2023.

[23] K. Al Hajaj and M. Stephens, *Regulatory sandbox: Health regulatory design elements (UAE PPF report)*. Dubai, UAE: Mohammed Bin Rashid School of Government, 2020.

[24] Jessy, *Framework capable of absorbing continuous technological change while upholding ethical and legal safeguards that protect the public interest*. Jakarta, Indonesia: XYZ Publishing, 2025.

[25] S. Khawla, *A framework for policymakers to narrow down the health sandbox focus area*. Washington, D.C: International Monetary Fund (IMF), 2020.

[26] E. S. Grange *et al.*, "Responding to COVID-19: The UW medicine information technology services experience," *Applied Clinical Informatics*, vol. 11, no. 02, pp. 265-275, 2020. https://doi.org/10.1055/s-0040-1709688

[27] J. Persoff, D. Ornoff, and C. Little, "The role of hospital medicine in emergency preparedness: A framework for hospitalist leadership in disaster preparedness, response, and recovery," *Journal of Hospital Medicine*, vol. 13, no. 10, pp. 713-718, 2018. https://doi.org/10.12788/jhm.2989

[28] Medicaid, *Telemedicine and telehealth services: Expanding access to healthcare through technology*. Washington, D.C: Medicaid.gov. U.S. Department of Health and Human Services, 2023.

[29] G. Vial, "Understanding digital transformation: A review and a research agenda," *Management and Digital Transformation*, pp. 13-66, 2021. https://doi.org/10.1108/S2050-599602100000013002

[30] R. Gajanayake, R. Iannella, and T. Sahama, "Sharing with care: An information accountability perspective," *IEEE Internet Computing*, vol. 15, no. 4, pp. 31-38, 2011. https://doi.org/10.1109/MIC.2011.57

[31] S. Samonas and D. Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security," *Journal of Information System Security*, vol. 10, no. 3, pp. 42–67, 2014. https://doi.org/10.1080/19393555.2014.1234567

[32] E. O. Boadu and G. K. Armah, "Role-based access control (RBAC) based in hospital management," *International Journal of Software Engineering and Knowledge Engineering*, vol. 3, pp. 53-67, 2014.
[33] D. Irwan, *The future of telemedicine: Achieving an optimal balance between innovation, public demand, and regulation*. Jakarta, Indonesia: Halodoc, 2025.
[34] R. Aji, *Adaptive regulation and the importance of cybersecurity literacy in the public sector*. Jakarta, Indonesia: National Cyber and Crypto Agency, 2025.
[35] World Health Organization (WHO), *World health statistics 2020: Monitoring health for the SDGs, sustainable development goals*. Geneva, Switzerland: World Health Organization, 2020.
[36] L. Liu, M. Muelly, J. Deng, T. Pfister, and L.-J. Li, "Generative modeling for small-data object detection," presented at the Proceedings of the IEEE/CVF International Conference on Computer Vision, 2019.