Lex Scientia Law Review
Vol. 9 Issue 2 (2025) 1668–1700
DOI: https://doi.org/10.15294/lslr.v9i2.12152
Online since: November 17, 2025

LEX SCIENTIA LAW REVIEW
https://journal.unnes.ac.id/journals/lslr

Toward an Effective Legal Framework for Digital Health E-Commerce: Insights from the UAE and Indonesia

Mourad Benseghir[a]✉, Maamar Bentria[b], Aoutef Zerara[c], Halima Bendriss [d], Badreddine Berrahlia[e].

[a] College of Law, University of Sharjah, UAE,

mbenseghir@sharjah.ac.ae, https://orcid.org/0000-0003-1943-2084
[b] College of Law, University of Sharjah, UAE,

mbentria@sharjah.ac.ae, https://orcid.org/0000-0003-2793-0024
[c] College of Law, University of Sharjah, UAE,

azerara@sharjah.ac.ae, https://orcid.org/0000-0002-2476-449X
[d] College of Law and Political Sciences, Djilali Liabes University of Sidi Bel Abbes, Algeria,

halima.bendriss@univ-sba.dz, https://orcid.org/0000-0003-1578-5552
[e] College of Law and Political Sciences, Badji Mokhtar - Annaba University,
Badreddine.berrahlia@univ-annaba.dz, https://orcid.org/0000-0002-8860-0304

✉ Corresponding email: mbenseghir@sharjah.ac.ae

Abstract

This study compares the regulatory frameworks of the United Arab Emirates (UAE) and Indonesia governing the online provision and

sale of health-related technologies. In technology-driven healthcare, data privacy and the security of digital transactions are central concerns. Employing a normative juridical approach, the research analyses applicable legislation, regulatory instruments, and scholarly literature in both jurisdictions. The findings indicate that the UAE has developed a relatively robust and comprehensive framework, particularly in relation to data protection and the security of digital health infrastructure, supported by detailed and stringent rules. By contrast, Indonesia's regulatory framework remains less effective in practice, hindered by limited public awareness of data security, uneven enforcement, and implementation challenges at the local and regional levels. The study underscores the key differences between the two systems and highlights the need, especially in Indonesia, for clearer, more enforceable rules on health-related online transactions and stronger safeguards for personal health data.

KEYWORDS *Legal Protection Digital Health E-Commerce, E-Commerce Regulation, Transparency, Accountability*

Introduction

Advances in information and communication technology have significantly expanded the ability of individuals to access and perform a wide range of medical tasks online. These innovations enable the rapid collection, organization, and exchange of health data, offering important advantages for patients, healthcare providers, and public health institutions. In many countries, the integration of electronic healthcare systems is expected to reduce healthcare costs, enhance the quality of care, and decrease the incidence of medical errors. By improving access to reliable information, digital health tools empower individuals to make better-informed decisions about their medical needs.[1]

At the same time, the increasing reliance on large-scale digital health infrastructures presents several urgent challenges. Effective public health surveillance, for instance, depends on the ability to analyze vast quantities of data quickly and accurately to detect emerging risks such as influenza outbreaks or adverse reactions to

[1] Giuseppe Aceto, Valerio Persico, and Antonio Pescape, "A Survey on Information and Communication Technologies for Industry 4.0: State-of-The-Art, Taxonomies, Perspectives, and Challenges," *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3467–3501, https://doi.org/10.1109/comst.2019.2938259.

medications. While digital systems can significantly strengthen these monitoring capabilities, they also heighten concerns regarding data accuracy, system reliability, and the protection of sensitive personal information. These issues underline the need for strong governance frameworks, advanced technological safeguards, and clear legal standards to ensure that the benefits of health technology can be realized without undermining public trust or patient safety.[2]

Healthcare providers and affiliated institutions routinely collect and store patient information within their digital systems to maintain accurate records and support future clinical decision-making. However, as these systems expand in scope and complexity, the stored data becomes increasingly vulnerable to unauthorized access or technological intrusions. Such vulnerabilities pose significant risks to patient confidentiality, data integrity, and overall public trust in digital health services.

These concerns highlight the importance of ensuring full compliance with regulatory requirements governing healthcare information systems. Potential privacy breaches, cybersecurity incidents, and other violations associated with the improper handling of digital health data underscore the need for robust legal safeguards and stringent oversight mechanisms. As the digital transformation of healthcare accelerates, rapid legislative adaptation becomes essential. Timely and effective regulatory reforms are not only necessary for addressing emerging risks but also for supporting the safe and sustainable growth of the e-health sector.[3]

The deployment of health technology in both the United Arab Emirates (UAE) and Indonesia faces several systemic challenges, particularly concerning data protection, patient confidentiality, product liability, and public trust. These issues have become increasingly urgent as both nations accelerate the digital transformation of their healthcare sectors and expand the use of e-health systems across public and private institutions.

In the UAE, concerns over personal data privacy and confidentiality constitute one of the most critical barriers to widespread adoption. Federal Law No. 2 of 2019 on the use of

---

[2] S. Briand, A. Mounts, and M. Chamberland, "Challenges of Global Surveillance during an Influenza Pandemic," *Public Health* 125, no. 5 (May 2011): 247–56, https://doi.org/10.1016/j.puhe.2010.12.007.

[3] Kirsten Martin, "The Penalty for Privacy Violations: How Privacy Violations Impact Trust Online," *Journal of Business Research* 82 (January 2018): 103–16, https://doi.org/10.1016/j.jbusres.2017.08.034.

Information and Communication Technology (ICT) in the healthcare sector imposes comprehensive obligations on healthcare providers, requiring them to ensure secure data storage, prevent unauthorized access, and comply with strict operational standards. However, despite this sophisticated legal framework, the rapid growth of electronic health records and digital platforms has increased the risk of breaches. The volume and sensitivity of health data held by both governmental and commercial entities make privacy protection a pressing national concern, heightening the need for continuous technological and regulatory vigilance.

Indonesia faces comparable risks but with even greater urgency. Although Law No. 27 of 2022 on Personal Data Protection (PDP) establishes a modern regulatory foundation, its practical implementation remains uneven. Persistent challenges, including limited public awareness, uneven technological infrastructure, and insufficient regulatory oversight, continue to undermine the effectiveness of the legal framework. The 2021 breach compromising the personal data of an estimated 279 million Indonesians underscored the vulnerability of health data systems and highlighted the immediate necessity for stronger enforcement mechanisms, investment in secure digital infrastructure, and improved institutional capacity.[4]

Another central barrier in both jurisdictions is product liability and public confidence in digital health tools. In the UAE, public trust is closely tied to the transparency of service providers, especially regarding how they mitigate risks of medical errors and ensure accountability when harm occurs.[5] Although the legal system offers relatively advanced protections, confidence can be weakened when liability boundaries are unclear. In Indonesia, the challenge is even more acute. Many e-health platforms are still emerging, and public unfamiliarity, coupled with gaps in legal safeguards and enforcement, requires authorities to adopt a more proactive approach through public education, clearer liability rules, and stringent monitoring of digital service providers.[6]

---

[4] Muhammad Yudistira and Ramadani Ramadani, "TINJAUAN YURIDIS TERHADAP EFEKTIVITAS PENANGANAN KEJAHATAN SIBER TERKAIT PENCURIAN DATA PRIBADI MENURUT UNDANG-UNDANG NO. 27 TAHUN 2022 OLEH KOMINFO," *UNES Law Review* 5, no. 4 (2022): 3917–29, https://doi.org/10.31933/unesrev.v5i4.698.

[5] Jawahitha Sarabdeen and Immanuel Azaad Moonesar, "Privacy Protection Laws and Public Perception of Data Privacy," *Benchmarking: An International Journal* 25, no. 6 (August 6, 2018): 1883–1902, https://doi.org/10.1108/bij-06-2017-0133.

[6] Abigail Prasetyo and Dyah Hapsari Prananingrum, "DISRUPSI LAYANAN KESEHATAN BERBASIS TELEMEDICINE: HUBUNGAN HUKUM DAN TANGGUNG JAWAB HUKUM

These issues, if not urgently addressed through comprehensive and well-coordinated policy reforms, risk limiting the transformative potential of health technology in expanding healthcare access and improving service quality. As Mahajan notes, weak data security directly undermines public willingness to use digital health systems, thereby reducing their overall effectiveness. [7]

To contextualize these challenges, it is instructive to consider the experiences of more developed jurisdictions. A 2006 U.S. survey showed that although 75 percent of physicians believed e-health could reduce medical errors and 70 percent believed it could enhance productivity, adoption rates remained low. Similar obstacles persist in many European countries, primarily due to insufficient legal protections surrounding privacy, cybersecurity, and liability. These global experiences show that robust legislation and strong governance structures are essential prerequisites for successful integration of health technologies.

Against this backdrop, this research pursues four main legal objectives, each addressing a critical dimension of e-health regulation:

1. Data privacy and confidentiality: Examining the adequacy of legal protections for personal health data in the UAE and Indonesia, and comparing them with frameworks in the US, UK, and EU.
2. Product liability: Analyzing legal accountability for harm caused by digital health tools, medical software, or algorithmic errors.
3. Judicial jurisdiction in e-health disputes: Exploring how courts determine jurisdiction in cases involving cross-border digital health services.
4. Professional negligence: Assessing how traditional medical negligence standards apply to healthcare providers who rely on digital tools or remote technologies.

This research adopts a comparative approach that incorporates relevant legal systems in the United States, the United Kingdom, and the European Union where appropriate. It addresses health technology in a broad sense, encompassing clinical services, decision-support systems, electronic medical information, and digital health-related commercial activities.

PASIEN DAN DOKTER," *Refleksi Hukum : Jurnal Ilmu Hukum* 6, no. 2 (June 8, 2022): 225–46, https://doi.org/10.24246/jrh.2022.v6.i2.p225-246.

[7] Hemant B. Mahajan, "Emergence of Healthcare 4.0 and Blockchain into Secure Cloud-Based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap," *Wireless Personal Communications* 126 (September 13, 2022): 2425–46, https://doi.org/10.1007/s11277-022-09535-y.

Method

This research employs a normative juridical methodology to examine and compare the regulatory frameworks governing health technology applications in digital healthcare systems in Indonesia and the United Arab Emirates (UAE). The study relies primarily on a detailed examination of binding legal instruments, such as statutes, implementing regulations, ministerial decrees, and governmental policy documents, relevant to both jurisdictions. These primary legal materials are supplemented with secondary sources, including academic literature, peer-reviewed journal articles, official institutional reports, and commentaries produced by regulatory agencies and international organizations.

Data collection is conducted through systematic library research, which involves several structured steps: (1) identifying relevant legal documents and scholarly sources; (2) categorizing them according to thematic relevance, such as privacy regulation, liability provisions, or digital-health governance; and (3) organizing these materials into an analytical framework suitable for cross-jurisdictional comparison. The data analysis process utilizes a qualitative-comparative technique, enabling the study to interpret legal concepts, evaluate the hierarchy and enforceability of rules, and identify both convergences and divergences between the Indonesian and UAE regulatory models.

To ensure the validity and reliability of the secondary data used in this research, the study applies source triangulation. This includes cross-checking information from multiple authoritative sources, such as government publications, official regulatory guidelines, and reputable academic journals, to confirm consistency and accuracy. Reliability is further strengthened by verifying that interpretations of legal norms are supported across different documents and by referencing internationally recognized standards in digital-health governance, ensuring that the assessment is grounded in established comparative legal principles.

Based on this methodological framework, the research aims to produce well-supported findings and strategic recommendations regarding the regulation of health technologies in digital healthcare environments in Indonesia and the UAE. These recommendations will highlight key areas requiring legal refinement and offer insights to guide future policy development.

Result & Discussion

A. Legal framework in health technology in E-Commerce in the UAE.

The objective of this analysis is to examine the legal framework that governs healthcare technology in e-commerce in the United Arab Emirates (UAE). [8] In light of the healthcare industry's ongoing digitization and technological advancements, it is imperative to understand how UAE laws are evolving to accommodate these developments. This research employs a normative juridical methodology, which entails the examination of laws, legal doctrine, and pertinent literature. The contemporary healthcare system is increasingly reliant on healthcare technology in e-commerce. To ensure the safe and efficient use of this technology, the UAE has enacted several laws. The present investigation will evaluate the practical application of the existing legal framework.

The law governing data protection To protect patients' personal information in digital healthcare, the UAE has implemented stringent data protection laws. The most recent draft of the UAE e-Privacy Regulations and the General Data Protection Regulation (GDPR), along with the recent data breach in the Middle East, indicate that the Gulf country would benefit from implementing specific local data protection and privacy regulations. The UAE Free Zones, including Dubai International Financial Centre, Abu Dhabi Public Market, and Dubai Health City, have implemented specific data protection regimes that are primarily based on and inspired by the privacy and data protection principles and guidelines outlined in the Data Protection Directive of 1995 and the Organisation for Economic Co-operation and Development (OECD) 1980 Guidelines on Privacy Protection and Cross-Border Flows of Personal Data. [9] However, the UAE has not yet implemented any unique federal data protection laws, which is a notable absence. In February 2019, the UAE President issued Federal Law No. 2 of 2019 (Health Data Law), which governs the use of information and communication technology in the healthcare sector. This is the first federal statute in the UAE that explicitly addresses data protection principles.

---

[8] Khalil Ibraheem Sh. Alshaikhi and Lemhannas RI, "Meningkatkan Kapasitas National Cybersecurity Authority (NCA) Kerajaan Arab Saudi Untuk Memperkuat Keamanan Digital Nasional" (Jakarta, Indonesia: Lemhannas RI (Lembaga Ketahanan Nasional Republik Indonesia), 2023), http://lib.lemhannas.go.id/public/media/catalog/0010-112300000000057/swf/7396/PPRA%2065%20-%2045%20s.pdf.

[9] Jawahitha Sarabdeen and Immanuel Azaad Moonesar, "Privacy Protection Laws and Public Perception of Data Privacy," *Benchmarking: An International Journal* 25, no. 6 (August 6, 2018): 1883–1902, https://doi.org/10.1108/bij-06-2017-0133.

The law incorporates well-known data protection concepts, including consent to disclosure, accuracy, security of measures, and limitation of purpose, in a manner that is analogous to the General Data Protection Regulation. What are the primary elements of the law? Processed data The Health Data Act regulates the processing of electronic health data that originates in the UAE. This data includes patient names, consultations, diagnosis and treatment data, alpha-numeric patient identifiers, general procedural technology codes, medical scan images, and lab results (health data). The legislation also introduces the well-known concepts of data privacy and protection. Accuracy is a critical concern for healthcare providers, as they are required to guarantee the reliability and accuracy of the processed health data. Unless the patient has provided prior consent, healthcare providers must limit the use of health data to the provision of healthcare services. Disclosure assent: Health service providers must obtain the patient's prior consent or legal permission before disclosing patient data to any third party. Measures to ensure security The use of appropriate security measures is required to ensure that health data is secure from unauthorised access, damage, alteration, deletion, or addition. [10]

Protection of data According to Article 4 of the Health Data Law, all health service providers who use information and communication technology to collect health data are required to maintain the confidentiality of the information and prevent its transfer without authorization. The law aligns with the security principles of the General Data Protection Regulation, which requires safeguarding health data from unauthorised damage, amendment, change, deletion, or addition to ensure its validity and credibility. Furthermore, the law mandates that health service providers guarantee access to health data and facilitate its use by authorized individuals. This encompasses restricting access to authorised personnel who comprehend the necessity of patient confidentiality. The Health Data Act mandates that entities establish technical, operational, and organisational procedures to guarantee the integrity and security of health data in compliance with international data protection standards and best practices. Data localization One of the most significant features of this new law will be a general prohibition on the transmission of health data outside the UAE, unless authorised by health-related authorities in coordination with government

[10] Siti Nur Eliza Rahmawati et al., "Privasi Dan Etika Dalam Manajemen Sumber Daya Manusia Digital," *Lokawati : Jurnal Penelitian Manajemen Dan Inovasi Riset* 1, no. 6 (October 3, 2023): 01-23, https://doi.org/10.61132/lokawati.v1i6.328.

ministries (Article 13). [11] This provision is an official representation of a longstanding unofficial regulatory policy that mandates the processing and storage of health data inside the United Arab Emirates (UAE). Practically speaking, the regulations would greatly affect enterprises that now depend on data storage or data processing solutions located outside the UAE, such as cloud or hosting services. Article 13 will have an equivalent effect on suppliers who are currently providing these services to the UAE. The law envisions specific exceptions to these data localization obligations, but they may only offer limited relief, [12] This will only occur in the future, namely in the next ministerial decision or implementing rule.

Data retention Article 20 mandates the retention of health data for a required duration, with a minimum of 25 years from the date of the patient's last operation. In this aspect, the Health Data Act differs from the GDPR, as the latter requires the retention of personal data only for the duration necessary for its processing. This poses a substantial compliance obligation for healthcare providers, who must guarantee that they possess the necessary skills and data storage systems to adhere to the requirements.

The implementation of Federal Law No. 2 of 2019 in the United Arab Emirates (UAE) has created significant practical challenges for healthcare providers, especially regarding the requirement that all health data must remain within the country. According to a PwC report, the law's strict prohibition on transferring patient data outside the UAE—unless special approval is granted—has forced many hospitals, clinics, and digital-health companies to re-evaluate how they store and manage information. [13] For example, several private hospitals that previously relied on international cloud services, such as servers located in Europe or the United States, were required to shift their entire data-storage systems to locally hosted platforms that comply with national rules. This transition has involved not only considerable financial investment, but also

---

[11] Erik Koornneef, Paul Robben, and Iain Blair, "Progress and Outcomes of Health Systems Reform in the United Arab Emirates: A Systematic Review," *BMC Health Services Research* 17, no. 1 (September 20, 2017), https://doi.org/10.1186/s12913-017-2597-1.

[12] Saleh Saad Alhubail, "Framework Data Modeling for the Proposed National Spatial Data Infrastructure of United Arab Emirates" (Technical Report No. 224, M.Eng. thesis, 2004), https://unbscholar.lib.unb.ca/bitstreams/4bbf91c0-c984-40c6-b6b1-0a0c2a2a5ad1/download.

[13] PWC (PwaterhouseCoopers), "Healthcare Data Protection in the UAE: A New Federal Law," PwC, 2019, https://www.pwc.com/m1/en/publications/healthcare-data-protection-in-the-uae.html.

operational adjustments such as redesigning IT networks, upgrading servers, and training staff to manage new systems.

Baker McKenzie notes that Ministerial Resolution No. 51/2021 provides a narrow exception allowing limited cross-border data transfers. However, using this exception in practice is far from simple. Healthcare providers must meet several detailed technical and administrative requirements, such as ensuring full data encryption, maintaining duplicate copies of all patient records inside the UAE, and documenting strict access-control procedures. [14]

In practical terms, this means that even if a healthcare provider uses an international telemedicine platform, they must keep a complete, secure copy of every patient file stored on servers physically located within the UAE. For smaller clinics or emerging digital-health start-ups, these compliance steps often increase operational costs and require specialized technical expertise.

These challenges illustrate that compliance with Federal Law No. 2 of 2019 is not only a legal obligation but also a substantial logistical undertaking. Healthcare institutions must adopt a comprehensive approach that includes upgrading technological infrastructure, investing in cybersecurity tools, and ensuring that personnel are adequately trained to manage sensitive data in accordance with national requirements. Without such adjustments, providers risk falling short of regulatory standards while also undermining the efficiency of their digital-health operations.

A centralized healthcare information technology system A centralised health data management system. The Ministry of Health and Prevention will direct the creation of a centralised health data management system. from health service providers and enable them to securely access and share this data in a standardised way, according to any government-imposed restrictions. Exemptions from limitations on revealing information According to Article 16, health service providers have the authority to use or reveal health data without obtaining the patient's permission.

Enables insurance companies and other organArticle 16 permits insurance companies and other medical care funding organizations to verify their financial rights for scientific research, provided they uphold patient anonymity and adhere to pertinent sciA

[14] Baker McKenzie Habib Al Mulla, "UAE: Health Data Law – Permitted Transfers of Health Data," Bakermckenzie.com (Baker McKenzie Insight+, July 2021), https://insightplus.bakermckenzie.com/bm/attachment_dw.action?attdocparam=pB7HEsg%2FZ312Bk8OIuOIH1c%2BY4beLEAegvKI1jun1HU%3D&attkey=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQJsWJiCH2WAVfnLVn2ghRGCra35vBpoQ%2B&fromContentView=1&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQbuwypnpZjc4%3D.

competent legal authority will request the implementation of public health measures for prevention and treatment. For the sake of public health, comply with requests from relevant health authorities, which may include conducting inspections. Penalties Any health authority conducting disciplinary proceedings may impose disciplinary measures and monetary fines as part of the Act's system of penalties for non-compliance. Sanctions may be levied, specifically for bThe Act specifically levies sanctions for breaches of data localization regulations. Ible suspension or revocation of the liThe license to access The relevant health authority may issue an official notification or admonition, accompanied by a fine ranging from AED 1,000 to AED 1,000,000.[15]

The Dubai Health Authority (DHA) introduced Administrative Decree Number 30 of 2017 to govern the provision of telehealth services in Dubai. However, the DHA recently revoked this rule. Subsequently, Dubai has seen a significant increase in the availability of telehealth services. [16] In 2019, Dubai Ruler HH Sheikh Mohammed bin Rashid Al Maktoum, the Vice President and Prime Minister of the UAE, announced the 'Fifty Year Charter' of Dubai, which contains nine articles that will determine the city's destiny. Article 5 aims to provide citizens with medical consultations through a global network of hundreds of thousands of physicians, experts, and medical advisors. [17]

Intelligent government apps will make this possible. We want to revolutionize healthcare by bringing physicians into the community, increasing public awareness of the importance of their work, and enlisting the help of world-renowned medical professionals to improve our residents' health. The DHA has made telehealth empowerment a top priority to meet the requirements of this clause. They have also implemented seven essential components to create

---

[15] Bryant Stokes, "Ministerial Review into the Public Health Response into the Adverse Events to the Seasonal Influenza Vaccine" (Perth, Australia: Government of Western Australia, Department of Health, 2010), https://www.health.wa.gov.au/~/media/Files/Corporate/Reports-and-publications/PDF/Stokes_Report.pdf.

[16] Khamis Al-Alawy and Immanuel Azaad Moonesar, "Perspective: Telehealth – beyond Legislation and Regulation," *SAGE Open Medicine* 11, no. 1 (January 2023): 205031212211432, https://doi.org/10.1177/20503121221143223.

[17] Saeed Al Mansoori, "From the Desert to the City: The Innovative Leadership of Sheikh Mohammed Bin Rashid al Maktoum, Vice President and Prime Minister of the United Arab Emirates (UAE) and Ruler of the Emirate of Dubai - ProQuest," *Proquest.com* (2018), https://www.proquest.com/openview/0a643c566196c31a6b5df0daec2d1df8/1?pq-origsite=gscholar&cbl=18750&diss=y.

a unique model for telehealth services, including providing medical consultations via telehealth. They have gained access to the patient's family tree through electronic heaWe prescribe pharmaceuticals using telemedicine, adhering to a registry of authorised pharmaceuticals prescribable through telehealth services. Emphasize the appropriate use of thermometers, glucose monitors, self-blood pressure monitors, and other vital indicators for early diagnosis. We have carefully examined all potential avenues for initiating a free telehealth services program. Create programs to encourage the use of telemedicine services and establish suitable regulations for their delivery in the Dubai Emirate. ubai Emirate.

In September 2019, the DHA issued the "Standards" for Telehealth Services. This standard lays out the very minimum that providers must meet in order to guarantee patient confidentiality and the delivery of high-quality telehealth services. Telehealth services include appointment scheduling, evaluations, guidance from medical professionals, treatment, therapy, lab testing, diagnosis, surgery, counseling, management of chronic conditions, and drug prescription and administration. This standard categorizes telehealth into six primary categories. Telemedicine encompasses a wide range of domains, including teleconsultation, telediagnosis, telemonitoring, health, telerobotics, and telepharmacy. [18] The DHA issues licences and gives special clearance to any healthcare facility or independent telehealth platform that wants to provide telehealth services. Categories for licensing telehealth services include: The DHA now recognizes the provision of telehealth services to various types of licenced health facilities. a telehealth facility that operates independently. Telehealth booths can be found at designated locations or on telehealth platforms. Telehealth services specifically do not cover emergency situations that require prompt action or referral due to potential life-threatening risks. Telehealth services do not cover the process of writing a prescription for a prohibited substance, narcotic, or semi-controlled substance. The platform is utilized for conducting in-person consultations, recording those consultations on video, and then storing those recorded videos. In accordance with these guidelines, clinicians may request to temporarily or ad hoc record video in writing for medical education and quality improvement purposes, thereby circumventing the general ban on video recording. To use telehealth services, each interaction necessitates the acquisition and documentation of

[18] Siddharth Singh et al., “Telemedicine, Telehealth, and E-Health: A Digital Transfiguration of Standard Healthcare System,” in *Cloud IoT* (USA: Chapman and Hall/CRC (Taylor & Francis Group), 2022).

consent. Either a paper copy or an electronic signature is DHA rules stipulate that only licenced doctors, nurses, and allied health professionals may provide telehealth services professionals who hold their licences from the DHA.

Confidentiality, data, and telehealth equipment in terms of data storage and transfer, the standard confirms compliance with Federal Law No. 2 of 2019 on the Use of ICT in the Health Sector. Within 18 months from the date of publication of the standard or licence, whichever comes later, from an internationally recognised accrediting authority for telehealth services, the UAE must repeat the topic of data localisation in 2019. [19] The Telecommunications Regulatory Authority's ('TRA') approval is a requirement for certain telehealth equipment, as stated in the standard. When evaluating any telehealth equipment, one should always consult the appropriate authorities and regulations, such as the Ministry of Health and Prevention for medical devices and the DHA for medical display screens.

The DHA requires the appointment of a responsible physician in the event of an AI-related medical error. It's unclear if the DHA would hold these doctors personally accountable for any AI medical mistakes, or if their role is merely to receive reports of mistakes and take corrective action. At least two weeks before allocating or relocating the telehealth booth, telehealth must acquire consent from the DHA. In addition to offering patients privacy while receiving telehealth services, the cubicle must also have a waiting space, following the minimal criteria for health clinics. Telehealth booths can't function independently. During operational hours, there must be at least one RN present in the cubicle, and accountable for the services offered, there must be at least one physician licenced by the DHA. [20]

Partner relationship management (PRM) may involve remote patient monitoring following an in-person evaluation at a healthcare institution or a virtual consultation. All information and communication technology (ICT) provided by relationship management partner providers must be in accordance with the Health Information and Communications Technology Act (HITECH),

---

[19] Amit Agrawal and Srinivas Kosgi, *Healthcare Access* (Norderstedt, Germany: BoD – Books on Demand, 2022).

[20] Betty Bügel Mogensen, Rossana Bossi, and Marianne Glasius, "Assessment of DHA in Self-Tanning Creams Applied in Spray Booths" (Copenhagen, Denmark: Danish Environmental Protection Agency (Ministry of Environment, Denmark), 2006), https://www2.mst.dk/udgiv/publications/2006/87-7052-235-9/pdf/87-7052-236-7.pdf.

the DHA interoperability standards, and the TRA. Drafting contracts and memoranda of understanding is necessary to use support services. It is the responsibility of the clinicians providing partner relationship management services to advise their patients about the use of monitoring devices that gather non-health-related data, such as patient location, and get their agreement before using these devices. Relationship Management Partner service providers must adhere to certain standards when collecting, using, and storing data, ensuring it is accurate, up-to-date, valid, and reliable. Additionally, they must promptly enter this data into the electronic health record.

The UAE Ministry of Health and Prevention's laws, the Health Information and Communication Technology Law, the National Electronic Security Authority (NESA), and the TRA all stipulate that health equipment must adhere to certain standardS. [21] Moreover, DHA mandates the submission of mobile health apps for evaluation and approval, among other additional criteria. Medical equipment used in telesurgery must be certified to comply with certain standards, such as those set forth by the FDA Quality System Regulations, the EU CE Marking, and the International Organisation for Standardisation (ISO) 9001 and ISO 9002. Telesurgery training is mandatory for clinicians, and it includes skills in force feedback (haptics), time delay, and depth perception management systems. Depending on the type of telesurgery, different robots and robotic systems may require distinct mechanical design classifications. It is important to employ the right medical equipment and instruments for each form of telesurgery, such as robot-assisted arms and arm trains, depending on the specialty. Some examples of these fields are urology, neurosurgery, gynaecology, cardiac, gastrointestinal, colorectal, spine, ophthalmology, and ear, neck, and throat.

In order to keep track of prescription shipments and handle customer payment data, telepharmacy service providers need an electronic pharmacy system. You cannot prescribe or administer controlled, semi-controlled, or narcotic drugs using telehealth services. One of the requirements for the issuance of prescriptions using an online prescription system is the electronic transmission of the prescription from the treating physician to the pharmacist or the patient uploading the prescription online. A order to legally operate as a pharmacy and engage in teledispensing, a licence from the Department of Health (DHA) is required. Teledispensing services are available for all drug varieties and prices. The Ministry of Health and

[21] Tanya Gibbs, "Seeking Economic Cyber Security: A Middle Eastern Example," *Journal of Money Laundering Control* 23, no. 2 (May 4, 2020): 493–507, https://doi.org/10.1108/jmlc-09-2019-0076.

Prevention must license medicine vending machines before they may provide over-the-counter goods and those on the general sales list. Only if a vending machine is located near or affiliated with a DHA-licensed pharmacy can it distribute medications and POMs. Telehealth has been a major focus for UAE authorities in 2019.

The impact of COVID-19 on medical treatment has been significant. In the years leading up to the COVID-19 pandemic, EHS has been using technology to enhance healthcare. Later,[22] during the COVID-19 pandemic, developers created additional applications to address the issue; however, many of these apps are now serving other purposes. So far, 1.7 million people have downloaded the app as of June 2022. During the epidemic, the app also offers virtual clinics, so users can speak with physicians from the comfort of their own homes. Now that people can move around more freely, these advancements remain in use. These days, it's all about making it easier for patients to get in touch with doctors, no matter where they are. In order to improve its forecasting capabilities, the UAE used AI and ML. Using this technique, EHS was able to forecast the spread of the pandemic and evaluate the dangers posed by COVID-19. By mining databases for patient information, they can predict which individuals pose the most danger, which ones are most likely to need hospitalisation, and so on. They can also predict the vaccination schedule and its distribution of hospital resources may be better anticipated with the use of these forecasts.

The implications of artificial intelligence and big data analytics are significant. Artificial intelligence (AI) and big data have become more important in UAE healthcare since the outbreak. Towards the beginning of 2023, [23] Abu Dhabi-based Presight AI signed a memorandum of understanding (MoU) with G42 Healthcare to develop underlying big data models. The partners will use Presight's omni-analytics platform and G42 Healthcare's healthcare industry expertise to create solutions for healthcare providers that simplify administrative practices, increase data accuracy, and reduce manual data entry. In addition, the partners' goal is to provide in-home services to people. They want to make better dietary, sleep, and

[22] M. Thaler et al., "Disruption of Joint Arthroplasty Services in Europe during the COVID -19 Pandemic: An Online Survey within the European Hip Society (EHS) and the European Knee Associates (EKA)," *Knee Surgery, Sports Traumatology, Arthroscopy* 28, no. 6 (May 2, 2020): 1712–19, https://doi.org/10.1007/s00167-020-06033-1.

[23] Sreejith Balasubramanian et al., "Applying Artificial Intelligence in Healthcare: Lessons from the COVID-19 Pandemic," *International Journal of Production Research* 63, no. 2 (October 3, 2023): 1–34, https://doi.org/10.1080/00207543.2023.2263102.

exercise recommendations and enhance early detection of health issues by integrating data acquired from smartwatches, wristbands, and sophisticated omics apps.

B. Indonesia's Legal Framework for Health Technology within the E-Commerce Ecosystem

Indonesia has a number of laws pertaining to electronic transactions and consumer protection, including Law No. 8 of 1999, Law of the Republic of Indonesia No. 11 of 2008, and Law of the Republic of Indonesia No. 7 of 2014, all found in the body of law known as "Law One article of the Trade Law that governs electronic trading networks states that all parties involved in the exchange of products or services must provide accurate and comprehensive data. Articles 65 and 66 of Chapter VIII, Trade Through Electronic Systems, govern the Trade Law's treatment of online trade. Meanwhile, the government continues to develop a regulation to address other aspects. A derivative of Government Regulation No. 82 of 2012, which deals with the implementation of electronic systems and transactions, outlines the responsibilities of operators of Indonesian electronic transaction systems in addition to the aforementioned e-commerce law. Operators of electronic transaction systems are required to comply with this government regulation.

Personal Data Protection Law No. 27 of 2022 has a close relationship with the health industry in Indonesia. The following key aspects shed light on this connection: Medical centres are required to follow certain protocols to safeguard their patients' private information, as outlined in the Personal Data Protection Act. Private information, including medical records, test results, and identifying details, is all part of this category of personal data.[24]

The implementation of regulations governing health technology and personal data protection within Indonesia's digital healthcare sector faces substantial challenges, especially at the local and regional levels. Although national laws such as the Personal Data Protection Law Law No. 27 of 2022 and the Minister of Health's regulations provide a legal foundation, their effectiveness varies

[24] Alaikha Annan, "Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022," *Synergy : Jurnal Ilmiah Multidisiplin* 1, no. 4 (2024): 247–54, https://e-journal.naureendigition.com/index.php/sjim/article/view/1040.

considerably across Indonesia's diverse regions due to differences in digital infrastructure, institutional capacity, and public digital literacy.

In many eastern regions, including Papua and Maluku, the adoption of telemedicine and health-related e-commerce platforms remains limited. Lukitawati and Novianto 2023 note that internet penetration in these provinces stands at approximately 47%, significantly below the national average of 77%. As a result, residents often struggle to access telemedicine applications, online pharmacy services, or electronic medical records. Several community health centers in Maluku, for example, reported interruptions in digital prescription systems due to unstable connectivity, forcing health workers to revert to manual processes. These disparities demonstrate that, despite national regulatory attempts to standardize digital health practices, limited local infrastructure hinders practical compliance and widens the healthcare gap between rural and urban populations.[25]

In contrast, major urban areas such as Jakarta and Surabaya demonstrate more advanced implementation of digital health regulations. Jakarta's Digital Health Center initiative enables patients to conduct online consultations and obtain digital prescriptions, which can be redeemed through registered pharmacies partnered with commercial e-health platforms. According to Prasetyo and Prananingrum 2022, public use of digital health services in Jakarta increased by 65% during the COVID-19 pandemic. This shows how regulatory frameworks, when supported by strong infrastructure and local governance, can facilitate innovation in health e-commerce. Nonetheless, the same study highlights persistent issues concerning patient-data protection, including unclear guidelines on data retention and inadequate monitoring of third-party digital platforms handling sensitive health information.[26]

Regulatory shortcomings also affect accountability within digital healthcare services. Annan 2024 reports that, due to the absence of clear rules on liability for telemedicine errors, many

[25] Hemant B. Mahajan, "Emergence of Healthcare 4.0 and Blockchain into Secure Cloud -Based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap," *Wireless Personal Communications* 126 (September 13, 2022): 2425–46, https://doi.org/10.1007/s11277-022-09535-y.

[26] Abigail Prasetyo and Dyah Hapsari Prananingrum, "DISRUPSI LAYANAN KESEHATAN BERBASIS TELEMEDICINE: HUBUNGAN HUKUM DAN TANGGUNG JAWAB HUKUM PASIEN DAN DOKTER," *Refleksi Hukum : Jurnal Ilmu Hukum* 6, no. 2 (June 8, 2022): 225–46, https://doi.org/10.24246/jrh.2022.v6.i2.p225-246.

consumer complaints remain unresolved. In West Java, for instance, complaints related to misdiagnosis through telemedicine platforms rose by 35% between 2021 and 2022. Local authorities often lack specific mechanisms to determine whether responsibility lies with the platform, the licensed medical practitioner, or the technology provider. This regulatory uncertainty directly affects health e-commerce companies, many of which struggle to establish clear risk-management procedures or standardized complaint-handling systems.[27]

These examples illustrate that insufficient regulatory enforcement at the regional level weakens the effectiveness of national laws and undermines public confidence in digital healthcare services. Without clear accountability standards, reliable oversight mechanisms, and adequate data-security safeguards, users may be reluctant to rely on digital health technologies, ultimately slowing the development of Indonesia's health e-commerce sector. Strengthening data-protection practices and clarifying liability rules are therefore essential steps toward building public trust and ensuring equitable access to digital healthcare across the country.

Patients' right to privacy and faith in medical professionals depend on this safeguard. To keep patients' private information safe, healthcare institutions must use appropriate security measures. This includes data encryption, access restrictions, and incident reporting in the event of a personal data breach.

Patients' informed consent is required before any data collection, use, or disclosure under the Personal Data Protection Act. This ensures that patients understand the use of their personal information and maintain control over it. With the implementation of the Personal Data Protection Law, healthcare institutions have a responsibility to guarantee the safety and dependability of their information technology systems. To avoid data breaches and unauthorised access, electronic medical record systems are required to fulfil certain security requirements. People will have more faith in digital health services if their data is well protected. Telemedicine and digital health consultations are examples of online health services that patients will feel more comfortable utilizing. Thus, the establishment of trustworthy health services in Indonesia is supported by the Personal Data Protection Law, which is vital in guaranteeing the secure management of patient personal data in line with set norms.[28]

---

[27] Annan, "Tinjauan Yuridis Perlindungan Data Pribadi,".

[28] Sandy Ekki Wiratama Buana, "Perlindungan Hukum Terhadap Data Pribadi Kepada

To raise the general level of health among Indonesians, Law No. 17 of 2023 was enacted. The following are some of the key features of this legislation: Rights and obligations. Make it clear what each person must and must do to get the health care they need. The provision of health care is a shared duty of the federal and state levels of government. This branch of health administration regulates health service facilities, health human resources, and health technology. By making them more resilient, make sure everyone can get their hands on drugs and medical gadgets. By overseeing their budgets, they keep health programs afloat. Encourage the community to participate in health improvement initiatives. This legislation aims to improve the quality of life in society, strengthen the national health system, and reduce health care inequities.

The Minister of Health Regulation No. 20 of 2019 regarding the implementation of telemedicine services does not directly mention health technology in online commerce.[29] This rule theoretically does not cover e-commerce, but it does govern telemedicine and other forms of remote health care that employ ICT. Telemedicine is defined as the delivery of long-distance health care by health professionals utilising information and communication technology. Article 1 is the one that matters for the tech-related aspects of telemedicine. Diagnosis, treatment, illness prevention, research, assessment, and CEU sharing all fall within this category. The Minister of Health Regulation No. 20 of 2019 defines telemedicine in Article 1 and includes several additional articles that are pertinent to health technology in e-commerce.[30]

Article 2 governs telemedicine services, including consultations, diagnoses, treatments, and remote health monitoring. Therefore, e-commerce service providers may offer a wide range of digital health services. Article 3 mandates that health care providers offering telemedicine services must possess qualifications and a valid practice permit. This guarantees that healthcare services offered via online marketplaces are of high quality and expertise. Article (4) establishes standards for the technical and operational aspects of

---

Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer to Peer Lending" (Master's thesis, 2022), https://dspace.uii.ac.id/handle/123456789/39314.

[29] Resita Lukitawati and Trisno Novianto Widodo, "Regulasi Layanan Kesehatan Digital Di Indonesia: Tantangan Etis Dan Hukum," *Ajudikasi: Jurnal Ilmu Hukum* 7, no. 2 (December 31, 2023): 391–414, https://doi.org/10.30656/ajudikasi.v7i2.7862.

[30] Abigail Prasetyo and Dyah Hapsari Prananingrum, "DISRUPSI LAYANAN KESEHATAN BERBASIS TELEMEDICINE: HUBUNGAN HUKUM DAN TANGGUNG JAWAB HUKUM PASIEN DAN DOKTER," *Refleksi Hukum : Jurnal Ilmu Hukum* 6, no. 2 (June 8, 2022): 225–46, https://doi.org/10.24246/jrh.2022.v6.i2.p225-246.

telemedicine, such as the use of trustworthy and secure information and communication technologies. 1. The security of patient information and the efficient operation of services depend on the Article 5 mandates that health care institutions offering telemedicine must have an integrated health information management system. 5. This allows for the integration of data from different health systems and e-commerce platforms, which improves service coordination and efficiency. Article 6 lays forth the rules that hospitals and other healthcare providers must follow to protect their patients' privacy and identity when they use telemedicine. This follows the guidelines set forth by the Personal Data Protection Act, which guarantee the appropriate security of patient data used in online transactions. These articles assist the growth of health technology in e-commerce in Indonesia by providing a clear and complete legal framework for the application of telemedicine. The regulation is number 20 of 2019 issued by the Minister of Health.

It is important to note that the objectives of health services utilizing information and communication technology must also comply with the provisions of laws and regulations. This is because Article 1, paragraph (3) of the 1945 Constitution of the Unitary State of the Republic of Indonesia asserts Indonesia's status as a legal state, thereby making the development of ICT-based health services, including telemedicine, a pertinent topic at present. Many ICT laws, including Article 28C, paragraph 1, of the 1945 Constitution, govern telemedicine. Health Law (No. 36/2009). The Medical Practice Law (No. 29/2004). Law No. 19/2016 modifies Law No. 11 of 2008, which deals with business and electronic transactions. Government Regulation No. 46/2014 pertains to health information systems. Hospital Law No. 44/2009. The Government's Health Service Facilities Regulation (No. 47/2016) is in effect. The Minister of Health issued Rule 269/2008, which relates to Health Records, and No. 2052/2011, which pertains to Medical Practice Permits and their implementation. The Minister of Health has issued Regulation No. 90/2015, which pertains to the provision of health services at health service facilities in extremely remote locations. The Ministerial Regulation No. 46/2017 pertains to the National e-Health Strategy.

Ministerial Regulation No. 20/2019 addresses the implementation of telemedicine between health care facilities. The Minister of Communication and Information issued Regulation No. 4/2016 on Information Security Management Systems. The Minister of Communication and Information also released Regulation No. 20/2016, which addresses the protection of personal data in

electronic health records. The Minister of Health issued Decree No. 409/2016, which pertains to trial hospitals for telemedicine services programs based on video conferencing and teleradiology. The Minister of Health issued Decree No. 650/2017 on the Organisation of Trials for Telemedicine Services by Hospitals and Community Health Centres. The Health Minister has issued Decree No. 4829/2021, which outlines Telemedicine Guidelines for the 2019 Coronavirus Disease (COVID-19) Pandemic. The Clinical Authority oversees Medical Practice through During the 2019 Coronavirus Disease (COVID-19) outbreak, the Indonesian Medical Council issued Regulation Number 74 of 2020. In Indonesia, in the context of COVID-19 prevention, Circular No. HK.02.01.MENKES/303/2020 discusses the use of information and communication technology for health service delivery. Titled "Regulation on the Implementation of Telemedicine Services between Health Service Facilities," Ministerial Regulation No. 20 of 2019 details the specific regulations that govern the use of telemedicine. Article 1, number 1, defines telemedicine as the delivery of health care by trained professionals utilizing electronic means of communication and remote locations.

Improved community and individual health is the goal of health information exchange, which encompasses a wide range of activities such as research, assessment, treatment, prevention, diagnosis, and continuing education for health care professionals. Furthermore, Article 3, paragraph (1) governs teleradiology, teleelectromagnetography, teleultrasonography, teleconsultation clinics, and other telemedicine consultation services that develop in tandem with scientific and technological advancements. Looking closer, however, we see that this system only governs telemedicine services provided from one health facility to another, by one health professional to another. Indeed, this regulation falls short of fully addressing all aspects of telemedicine in Indonesia. This includes both its use in times of crisis (disasters, pandemics, etc.) and its use through an e-health platform, specifically an app that connects patients and doctors. Therefore, we cannot rely on it as a blueprint for the complete implementation of telemedicine in Indonesia.[31]

A lack of regulations may have far-reaching effects on people's ability to have their data protected. An all-encompassing framework is required to control the internet economy, as shown by the rapid expansion of e-commerce in Indonesia. The government must safeguard citizens against fraudsters who prey on the surge in online payments, promote robust e-governance, and foster a society

[31] Lukitawati and Widodo, “Regulasi Layanan Kesehatan Digital Di Indonesia,”.

where everyone has access to digital tools.

This includes digital health. A lack of oversight by governments may potentially affect digital health. Digital health assets, such as interesting video-based health teaching resources, are a boon to frontline health workers in Papua, for instance. However, there isn't enough support in place; digital projects haven't taken into account the broader socio-cultural practices that impact frontline workers' employment, and digital frameworks haven't changed to accommodate their demands. Consider the ongoing challenges faced by community health care workers. These include language obstacles, societal stigma linked to HIV status, and power dynamics within communities that grapple with caste and gender hierarchies, among other things. This implies that healthcare facilities should follow established protocols to clarify data collection and its purpose for patients. One way to ensure that informed consent is actualized in a way that guarantees the right to autonomy and protects personal rights is to adopt a rights-based framework that takes into account the unique needs of marginalised communities. This framework should be sensitive to socio-economic conditions and privacy rights. The framework should also take into account the individual's right to privacy and secrecy. The next section delves into the difficulties associated with privacy.

C. Ideal Legal Framework for Regulating Health Technology in Indonesia’s E-Commerce Sector: Lessons from the UAE Model

In this age of rapid technological advancement, health technology has become an essential component of online commerce throughout all regions of Indonesia, including. Telemedicine, online health consultations, and the sale of medications via digital platforms are just a few examples of the many services that include this technology. To guarantee the safety, confidentiality, and excellence of healthcare services, however, a transparent legislative framework is necessary to keep up with this rapid evolution. Since the UAE has been so successful in establishing thorough laws in this area, Indonesia might study its regulatory notions to design an optimal legal framework.

The government of Indonesia has published many rules to control digital health services, beginning with policies and regulations. An essential measure is the Ministry of Health's establishment of the Regulatory Sandbox, which provides a controlled setting for the testing of digital health advances before their widespread introduction. This aids in the detection and

resolution of any ethical and legal concerns. One of them is the fact that the Ministry of Health has never before offered legal protection to a health-related digital technology development. Up until now, developers have only received protection through cooperation agreements. The next natural issue is how the government can shield very disruptive digital technologies from regulatory scrutiny. What procedures does the Ministry of Health need to put in place to ensure that regular education, mentoring, and testing are carried out? There are well-founded concerns that the public and the ecosystem's trust in digital health innovation will not flourish until this issue is resolved promptly. Consequently, rules governing the health care industry need a fresh strategy to keep up with the lightning-fast pace of digital innovation. The current regulatory environment should focus attention on the challenge of controlling innovation without stifling it due to excessive complexity and rigidity.

However, as the public may be enticed to engage, co-create, or even support each invention, the government must discover new regulatory possibilities or enhancements. There are rules in place to control technological innovation in Indonesia; they call it the regulatory sandbox. Since its implementation in 2018, the Financial Services Authority (OJK) has maintained a regulatory sandbox that only addresses financial technology.

Regulatory sandboxes serve multiple purposes, such as (1) facilitating the rapid and accurate testing of regulations in response to real-world conditions, (2) connecting developers in the digital health industry with health regulators, and (3) assuring investors that their money will be well-spent in telemedicine startups. Thus, to foresee developments that might threaten the telemedicine industry, a regulatory sandbox is required. The ongoing digital revolution in every country encourages people to adjust to current advancements. While each country's digital transformation scenario is unique, there is a general upward trend in internet adoption and the shift from offline to online activity. The 2020 survey by WeAreSocial and Hootsuite found that there were 4.54 billion internet users, or 59% of the population. Among Southeast Asian countries, 66% of the population has access to the internet, and 135% of that figure has mobile data connections, according to regional statistics.[32]

[32] Samanta Kocijan, Ana Globocnik Zunac, and Petra Ercegovac, "Changes to Social Patterns of Behaviour Stimulated by the Development of ICT and Digital Transformation" (60th International Scientific Conference on Economic and Social Development – XX International Social Congress (ISC 2020), Moscow, Russia: Economic and Social Development: Book of Proceedings, 2020), 1–9, https://www.bib.irb.hr:8443/1095944/download/1095944.Book_of_Proceedings_es

According to these geographical statistics, South-east Asia is among the world's most digitally transformed areas. This growing tendency is putting pressure on regional and municipal governments to control digital transformation by establishing both primary and secondary legislation.

For the sandbox to function effectively, its operational design must include explicit technical criteria. Participants—whether telemedicine companies, health-tech startups, or digital pharmacy platforms, should meet minimum technology, readiness standards, including secure data-processing capabilities, stable system architecture, and the ability to comply with data-protection protocols. Alami et al. (2020) note[33] that successful sandboxes rely heavily on transparent selection processes and rigorous evaluation mechanisms. In the Indonesian context, this means establishing clear procedural rules such as:

1. Detailed guidelines on data collection, storage, and use;
2. mandatory anonymization and strong encryption techniques for patient data;
3. Real-time reporting obligations to regulatory authorities;
4. System resilience testing to evaluate reliability under local connectivity conditions.

These requirements are particularly important given Indonesia's heightened vulnerability to data breaches and inconsistent cybersecurity practices in the health sector. By embedding these safeguards within the sandbox structure, Indonesia can simultaneously enhance innovation and reduce the risks associated with premature or unsafe deployment of digital health services.

Another essential component is independent oversight. The sandbox should not operate solely under government supervision but must involve universities, medical associations, and international independent bodies to serve as periodic auditors. As Ooi and Tan (2022) argue, the presence of impartial external evaluators improves the objectivity of assessments and strengthens public trust, an essential element for the long-term adoption of digital health technologies in Indonesia.[34]

In this regard, examining the UAE's regulatory experience

---

dMoscow2020_Online.pdf#page=10.

[33] Toddy Aditya and Achmad Chumaedi, "Digital Gap in Public Services to Support Development in the Coastal Area of Tangerang Regency," *Jurnal Humanitas Katalisator Perubahan Dan Inovator Pendidikan* 10, no. 4 (December 31, 2024): 600–619, https://doi.org/10.29408/jhm.v10i4.27350.

[34] Fatih Aydin and Cem Hakan Başaran, "Blockchain Revolution: Transforming Digital Health for a Secure Future" (Academic Press, 2025), 475–502, https://doi.org/10.1016/B978-0-443-30168-1.00017-7.

remains valuable, not as a model to be replicated wholesale, but as a comparative reference. Lessons from the UAE can guide Indonesia in building a sandbox framework that is realistic, locally adapted, and aligned with international standards for patient-data protection and digital health quality assurance. By tailoring the model to Indonesia's infrastructural and socio-cultural landscape, regulators can create a more inclusive, secure, and sustainable ecosystem for the development of health technologies in the e-commerce sector.

The United Arab Emirates' Ministry of Health and Prevention (MOHAP) and the Dubai Health Authority (DHA) vigorously oversee digital health legislation.[35] To make sure digital health services are safe, good, and effective, these groups have set up a complete framework. Here are a few important points and rules set down by law. The Health Care Information Technology Act of 2019 (No. 2 of the Federal Laws) is a key piece of legislation. All areas of the United Arab Emirates, including free zones, are subject to this legislation, known as the Information and Communication Technology Health Act, which governs the use of ICT in healthcare. That is the primary goal of this statute.

Optimal Information and Communication Technology Utilization: Make sure that the health sector is making good use of ICT to enhance service delivery. Local practices align with globally recognised standards to guarantee quality and safety. Data Security: Guard against unauthorised access to protected health information. 1. Centralised Health Data Exchange: Create a Ministry-run system to exchange health records in a standardised and safe way so that medical professionals may share patient records.

In the next section, we will address issues related to data protection and privacy. Our legal structure primarily tackles this issue. The collection, storage, and use of personal data by digital health service providers in Indonesia is governed by the Personal Data Protection Law.[36] Ensuring the preservation of patient privacy and preventing data exploitation is of utmost importance. There are several major obstacles to the health sector's Personal Data Protection Law. Some of the most significant challenges in addressing cyber threats and ensuring data security include the following: because of its immense value and extreme sensitivity, health data is a popular target for hackers. Cyberattacks such as

[35] Khawla Eissa Alhajaj and Immanuel Azaad Moonesar, "The Power of Big Data Mining to Improve the Health Care System in the United Arab Emirates," *Journal of Big Data* 10, no. 1 (February 1, 2023), https://doi.org/10.1186/s40537-022-00681-5.

[36] Yudistira and Ramadani, "TINJAUAN YURIDIS TERHADAP EFEKTIVITAS PENANGANAN KEJAHATAN SIBER TERKAIT PENCURIAN DATA PRIBADI,".

ransomware and data theft may result in patient data breaches. For example, in 2021, hacker forums allegedly saw the sale of data belonging to 279 million Indonesians. In terms of implementation and compliance, several healthcare institutions are currently struggling to meet the requirements of the Personal Data Protection Law. We can implement sufficient security measures such as data encryption and access restrictions for authorised users. A common obstacle to successful implementation is a lack of necessary resources as well as technical expertise. After that, we have data fragmentation; the federal and provincial governments of Indonesia have created over 400 health apps.[37] This fragmentation complicates data integration and interchange, potentially impeding comprehensive data-driven health strategies. This further complicates matters when trying to guarantee that all apps adhere to the same data security regulations.

The Dubai Data Law and Federal Law No. 2 of 2019 on the Use of Information and Communication Technology in the Health Sector are two of the most important laws in the United Arab Emirates (UAE) that govern the security of healthcare data.[38] These rules guarantee that medical records are secure and handled correctly. The following is an in-depth description: 1. Data Law in Dubai. Dubai enacted the Dubai Data Law to regulate data exchange, use, and repurposing. A safe and effective method for exchanging data is the goal of this statute. Some important factors are: Obligation to Share Data: Secure and mutually beneficial data sharing between the public and commercial sectors is a legal requirement. Information security mandates stringent data protection requirements to guarantee the utmost privacy and security for any information exchanged. Guidelines and Requirements: In order to keep data safe and secure, entities must follow certain rules and regulations. The Code of Federal Regulations No. 2 of 2019 governs the application of Electronic Health Records. This legislation, also known as the Information and Communication Technology Health legislation, governs the use of ICT in healthcare in the United Arab Emirates (UAE), including free zones. Efficient ICT utilization is one of the primary goals and stipulations of this statute.

---

[37] Mochamad Reiza Adiyasa and Meiyanti Meiyanti, "Pemanfaatan Obat Tradisional Di Indonesia: Distribusi Dan Faktor Demografis Yang Berpengaruh," *Jurnal Biomedika Dan Kesehatan* 4, no. 3 (September 30, 2021): 130–38, https://doi.org/10.18051/jbiomedkes.2021.v4.130-138.

[38] Manoj Kumar M V et al., "ICT Enabled Disease Diagnosis, Treatment and Management—a Holistic Cost-Effective Approach through Data Management and Analysis in UAE and India," *Frontiers in Artificial Intelligence* 5 (June 16, 2022): 909101, https://doi.org/10.3389/frai.2022.909101.

Make sure you're using healthcare IT effectively to improve patient outcomes. Global benchmark. Local procedures should align with globally recognised standards to guarantee quality and safety. Protect sensitive medical records and patient information. Health Data Exchange in One Place: The Ministry of Health and Prevention should establish a centralised system for health data interchange to ensure the safe and consistent transfer of patient information. The Health Assistance in Communications and Technology Act imposes crucial requirements. Respect for privacy. Healthcare practitioners must maintain the confidentiality of all patient information without appropriate authorization. We achieve data integrity by preventing accidental or malicious alteration, deletion, or loss of sensitive health information, and by guaranteeing its accuracy and reliability. Managed Access. Make sure that only authorized individuals can access health data, and make it easier for them to do so when needed. Setting up and adhering to regulations The United Arab Emirates has set up systems for monitoring and enforcing compliance with these rules.

This includes regular audits, certification, and penalties for noncompliance. Updates and changes can easily adjust the regulatory framework to accommodate new technologies. A Study of the UAE's Method: Indonesia could learn from the UAE's approach to digital health regulation. Indonesia can enhance its digital health ecosystem and guarantee the service's innovation and safety. Some examples are: Creating an Unambiguous Legal Structure. The Information and Communication Technology Health Law may serve as a model for Indonesia's legislative development to regulate the use of ICT in healthcare. Implement stringent data protection procedures to safeguard patient information and guarantee data protection. One of them is the creation of transparent criteria for digital health services to follow to ensure they are up to par. Establish robust systems to monitor compliance and ensure adherence to the rules.

Conclusion

According to these findings, the United Arab Emirates has established a legislative framework that facilitates the better use of health technology in online commerce. This is exemplified by the preparedness of sufficient digital infrastructure and the enforcement of stringent legislation about data privacy and security. Strong data privacy legislation, substantial investment in ICT, and active government participation in health tech monitoring and

implementation are some of the main reasons for the UAE's success. On the other hand, establishing a sufficient legislative framework for health technology in e-commerce remains difficulty in Indonesia. Inadequate technical infrastructure, a lack of legislation governing health e-commerce, and limited public understanding of the significance of data security and privacy are all obstacles. As a result, there are security holes and hazards associated with protecting personal data.

These results lead to several important conclusions. The first is the critical need for a robust legislative framework that guarantees data privacy and innovation in health e-commerce. Second, increased international collaboration should establish worldwide standards for health e-commerce. This will help unify security and data protection policies. Future studies should further explore methods to ensure the secure and effective implementation of health technology, as well as the impact of various nations' legislative regulations on the availability of digital health services. The recommendations for Indonesia include a public education campaign to raise awareness about the significance of personal data security in e-commerce, the development and updating of regulations related to health e-commerce, and the involvement of industry stakeholders in policy dialogue to guarantee that regulations encourage innovation while safeguarding consumers.

References

Aceto, Giuseppe, Valerio Persico, and Antonio Pescape. “A Survey on Information and Communication Technologies for Industry 4.0: State-of-The-Art, Taxonomies, Perspectives, and Challenges.” *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3467–3501. https://doi.org/10.1109/comst.2019.2938259.

Aditya, Toddy, and Achmad Chumaedi. “Digital Gap in Public Services to Support Development in the Coastal Area of Tangerang Regency.” *Jurnal Humanitas Katalisator Perubahan Dan Inovator Pendidikan* 10, no. 4 (December 31, 2024): 600–619. https://doi.org/10.29408/jhm.v10i4.27350.

Adiyasa, Mochamad Reiza, and Meiyanti Meiyanti. “Pemanfaatan Obat Tradisional Di Indonesia: Distribusi Dan Faktor Demografis Yang Berpengaruh.” *Jurnal Biomedika Dan Kesehatan* 4, no. 3 (September 30, 2021): 130–38. https://doi.org/10.18051/jbiomedkes.2021.v4.130-138.

Agrawal, Amit, and Srinivas Kosgi. *Healthcare Access*. Norderstedt, Germany: BoD – Books on Demand, 2022.

Al Mansoori, Saeed. “From the Desert to the City: The Innovative

Leadership of Sheikh Mohammed Bin Rashid al Maktoum, Vice President and Prime Minister of the United Arab Emirates (UAE) and Ruler of the Emirate of Dubai - ProQuest." *Proquest.com*, 2018. https://www.proquest.com/openview/0a643c566196c31a6b5df0daec2d1df8/1?pq-origsite=gscholar&cbl=18750&diss=y.

Al-Alawy, Khamis, and Immanuel Azaad Moonesar. "Perspective: Telehealth – beyond Legislation and Regulation." *SAGE Open Medicine* 11, no. 1 (January 2023): 205031212211432. https://doi.org/10.1177/20503121221143223.

Alhajaj, Khawla Eissa, and Immanuel Azaad Moonesar. "The Power of Big Data Mining to Improve the Health Care System in the United Arab Emirates." *Journal of Big Data* 10, no. 1 (February 1, 2023). https://doi.org/10.1186/s40537-022-00681-5.

Alhubail, Saleh Saad. "Framework Data Modeling for the Proposed National Spatial Data Infrastructure of United Arab Emirates." Technical Report No. 224, M.Eng. thesis, 2004. https://unbscholar.lib.unb.ca/bitstreams/4bbf91c0-c984-40c6-b6b1-0a0c2a2a5ad1/download.

Alshaikhi, Khalil Ibraheem Sh., and Lemhannas RI. "Meningkatkan Kapasitas National Cybersecurity Authority (NCA) Kerajaan Arab Saudi Untuk Memperkuat Keamanan Digital Nasional." Jakarta, Indonesia: Lemhannas RI (Lembaga Ketahanan Nasional Republik Indonesia), 2023. http://lib.lemhannas.go.id/public/media/catalog/0010-112300000000057/swf/7396/PPRA%2065%20-%2045%20s.pdf.

Annan, Alaikha. "Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022." *Synergy : Jurnal Ilmiah Multidisiplin* 1, no. 4 (2024): 247–54. https://e-journal.naureendigition.com/index.php/sjim/article/view/1040.

Aydin, Fatih, and Cem Hakan Başaran. "Blockchain Revolution: Transforming Digital Health for a Secure Future," 475–502. Academic Press, 2025. https://doi.org/10.1016/B978-0-443-30168-1.00017-7.

Baker McKenzie Habib Al Mulla. "UAE: Health Data Law – Permitted Transfers of Health Data." Bakermckenzie.com. Baker McKenzie Insight+, July 2021. https://insightplus.bakermckenzie.com/bm/attachment_dw.action?attdocparam=pB7HEsg%2FZ312Bk8OIuOIH1c%2BY4beLEAegvKI1jun1HU%3D&attkey=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQJsWJiCH2WAVfnLVn2ghRGCra35vBpoQ%2B&

fromContentView=1&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQbuwypnpZjc4%3D.

Balasubramanian, Sreejith, Vinaya Shukla, Nazrul Islam, Arvind Upadhyay, and Linh Duong. "Applying Artificial Intelligence in Healthcare: Lessons from the COVID-19 Pandemic." *International Journal of Production Research* 63, no. 2 (October 3, 2023): 1–34. https://doi.org/10.1080/00207543.2023.2263102.

Briand, S., A. Mounts, and M. Chamberland. "Challenges of Global Surveillance during an Influenza Pandemic." *Public Health* 125, no. 5 (May 2011): 247–56. https://doi.org/10.1016/j.puhe.2010.12.007.

Buana, Sandy Ekki Wiratama. "Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer to Peer Lending." Master's thesis, 2022. https://dspace.uii.ac.id/handle/123456789/39314.

Gibbs, Tanya. "Seeking Economic Cyber Security: A Middle Eastern Example." *Journal of Money Laundering Control* 23, no. 2 (May 4, 2020): 493–507. https://doi.org/10.1108/jmlc-09-2019-0076.

Kocijan, Samanta, Ana Globocnik Zunac, and Petra Ercegovac. "Changes to Social Patterns of Behaviour Stimulated by the Development of ICT and Digital Transformation," 1–9. Moscow, Russia: Economic and Social Development: Book of Proceedings, 2020. https://www.bib.irb.hr:8443/1095944/download/1095944.Book_of_Proceedings_esdMoscow2020_Online.pdf#page=10.

Koornneef, Erik, Paul Robben, and Iain Blair. "Progress and Outcomes of Health Systems Reform in the United Arab Emirates: A Systematic Review." *BMC Health Services Research* 17, no. 1 (September 20, 2017). https://doi.org/10.1186/s12913-017-2597-1.

Kumar M V, Manoj, Jagadish Patil, K. Aditya Shastry, Shiva Darshan, Nanda Kumar Bidare Sastry, Immanuel Azaad Moonesar, Shadi Atalla, Nasser Almuraqab, and Ananth Rao. "ICT Enabled Disease Diagnosis, Treatment and Management—a Holistic Cost-Effective Approach through Data Management and Analysis in UAE and India." *Frontiers in Artificial Intelligence* 5 (June 16, 2022): 909101. https://doi.org/10.3389/frai.2022.909101.

Lukitawati, Resita, and Trisno Novianto Widodo. "Regulasi Layanan Kesehatan Digital Di Indonesia: Tantangan Etis Dan Hukum." *Ajudikasi: Jurnal Ilmu Hukum* 7, no. 2 (December 31, 2023): 391–414. https://doi.org/10.30656/ajudikasi.v7i2.7862.

Mahajan, Hemant B. "Emergence of Healthcare 4.0 and Blockchain into Secure Cloud-Based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap." *Wireless Personal Communications* 126 (September 13, 2022): 2425–46. https://doi.org/10.1007/s11277-022-09535-y.
Mahajan, Hemant B. "Emergence of Healthcare 4.0 and Blockchain into Secure Cloud-Based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap." *Wireless Personal Communications* 126 (September 13, 2022): 2425–46. https://doi.org/10.1007/s11277-022-09535-y.
Martin, Kirsten. "The Penalty for Privacy Violations: How Privacy Violations Impact Trust Online." *Journal of Business Research* 82 (January 2018): 103–16. https://doi.org/10.1016/j.jbusres.2017.08.034.

Mogensen, Betty Bügel, Rossana Bossi, and Marianne Glasius. "Assessment of DHA in Self-Tanning Creams Applied in Spray Booths." Copenhagen, Denmark: Danish Environmental Protection Agency (Ministry of Environment, Denmark), 2006. https://www2.mst.dk/udgiv/publications/2006/87-7052-235-9/pdf/87-7052-236-7.pdf.

Prasetyo, Abigail, and Dyah Hapsari Prananingrum. "DISRUPSI LAYANAN KESEHATAN BERBASIS TELEMEDICINE: HUBUNGAN HUKUM DAN TANGGUNG JAWAB HUKUM PASIEN DAN DOKTER." *Refleksi Hukum : Jurnal Ilmu Hukum* 6, no. 2 (June 8, 2022): 225–46. https://doi.org/10.24246/jrh.2022.v6.i2.p225-246.
Prasetyo, Abigail, and Dyah Hapsari Prananingrum. "DISRUPSI LAYANAN KESEHATAN BERBASIS TELEMEDICINE: HUBUNGAN HUKUM DAN TANGGUNG JAWAB HUKUM PASIEN DAN DOKTER." *Refleksi Hukum : Jurnal Ilmu Hukum* 6, no. 2 (June 8, 2022): 225–46. https://doi.org/10.24246/jrh.2022.v6.i2.p225-246.

Prasetyo, Abigail, and Dyah Hapsari Prananingrum. "DISRUPSI LAYANAN KESEHATAN BERBASIS TELEMEDICINE: HUBUNGAN HUKUM DAN TANGGUNG JAWAB HUKUM PASIEN DAN DOKTER." *Refleksi Hukum : Jurnal Ilmu Hukum* 6, no. 2 (June 8, 2022): 225–46. https://doi.org/10.24246/jrh.2022.v6.i2.p225-246.
PWC (PwaterhouseCoopers). "Healthcare Data Protection in the UAE: A New Federal Law." PwC, 2019. https://www.pwc.com/m1/en/publications/healthcare-data-protection-in-the-uae.html.

Rahmawati, Siti Nur Eliza, Hasanah Maulinda, Rohmah Ainur, Adytia

Putra Pratama Rizki, and M Isa Anshori. "Privasi Dan Etika Dalam Manajemen Sumber Daya Manusia Digital." *Lokawati : Jurnal Penelitian Manajemen Dan Inovasi Riset* 1, no. 6 (October 3, 2023): 01-23. https://doi.org/10.61132/lokawati.v1i6.328.

Sarabdeen, Jawahitha, and Immanuel Azaad Moonesar. "Privacy Protection Laws and Public Perception of Data Privacy." *Benchmarking: An International Journal* 25, no. 6 (August 6, 2018): 1883–1902. https://doi.org/10.1108/bij-06-2017-0133.

Sarabdeen, Jawahitha, and Immanuel Azaad Moonesar. "Privacy Protection Laws and Public Perception of Data Privacy." *Benchmarking: An International Journal* 25, no. 6 (August 6, 2018): 1883–1902. https://doi.org/10.1108/bij-06-2017-0133.

Singh, Siddharth, Pankaj Kumar, Faisal Rehman, and Poonam Vashishta. "Telemedicine, Telehealth, and E-Health: A Digital Transfiguration of Standard Healthcare System." In *Cloud IoT*. USA: Chapman and Hall/CRC (Taylor & Francis Group), 2022.

Stokes, Bryant. "Ministerial Review into the Public Health Response into the Adverse Events to the Seasonal Influenza Vaccine." Perth, Australia: Government of Western Australia, Department of Health, 2010. https://www.health.wa.gov.au/~/media/Files/Corporate/Reports-and-publications/PDF/Stokes_Report.pdf.

Thaler, M., Ismail Khosravi, M. T. Hirschmann, N. P. Kort, L. Zagra, J. A. Epinette, and M. C. Liebensteiner. "Disruption of Joint Arthroplasty Services in Europe during the COVID-19 Pandemic: An Online Survey within the European Hip Society (EHS) and the European Knee Associates (EKA)." *Knee Surgery, Sports Traumatology, Arthroscopy* 28, no. 6 (May 2, 2020): 1712–19. https://doi.org/10.1007/s00167-020-06033-1.

Yudistira, Muhammad, and Ramadani Ramadani. "TINJAUAN YURIDIS TERHADAP EFEKTIVITAS PENANGANAN KEJAHATAN SIBER TERKAIT PENCURIAN DATA PRIBADI MENURUT UNDANG-UNDANG NO. 27 TAHUN 2022 OLEH KOMINFO." *UNES Law Review* 5, no. 4 (2022): 3917–29. https://doi.org/10.31933/unesrev.v5i4.698.

***

Acknowledgment
None

Funding Information
None

Conflicting Interest Statement
There is no conflict of interest in the publication of this article.

History of Article
Submitted : August 18, 2024
Revised : May 10, 2025
Accepted : July 17, 2025
Published : November 17, 2025