Research Article

Legal Guarantees for the Protection of Patient Confidentiality: A Cross-Jurisdictional Study

Mourad Benseghir*, Maamar Bentria, Adnan Ibrahim Sarhan, Salih Ahmed Luhaibi, Alaa Yakoob Yousif
College of Law, University of Sharjah, United Arab Emirates
***mbenseghir@sharjah.ac.ae**

ABSTRACT

This study examines the legal guarantees governing the confidentiality of patient information in Indonesia and the United Arab Emirates (UAE), two jurisdictions undergoing rapid digital transformation in their healthcare sectors. As the adoption of electronic medical records, telemedicine, and health information systems expands, concerns surrounding the protection, governance, and misuse of patient information have intensified. Through a normative and comparative legal method, this research analyzes the primary legislative instruments, regulatory mechanisms, and institutional arrangements that safeguard patient confidentiality in both countries. The UAE has established a more unified and structured legal framework, particularly through Federal Law No. 2 of 2019 on the Use of Information and Communication Technology (ICT) in Health Fields and the Personal Data Protection Law No. 45 of 2021, which impose stringent obligations for secure processing, access limitation, and data governance. Indonesia, on the other hand, has introduced key regulations such as the Health Law No. 17 of 2023, Minister of Health Regulation No. 24 of 2022 on Medical Records, and the Personal Data Protection Law No. 27 of 2022; however, challenges persist in enforcement consistency, system interoperability, and institutional capacity. By comparing legal standards, confidentiality obligations, penalties for violations, and enforcement practices, this study highlights the strengths and weaknesses of both frameworks. The findings underscore the need for Indonesia to enhance regulatory coherence, improve oversight mechanisms, and adopt best-practice elements from the UAE to reinforce patient information protection.

Keywords: Patient Confidentiality; Patient Information Protection; Comparative Health Legislation; Indonesia; United Arab Emirates.

A. INTRODUCTION

Recent innovations driven by information and communication technology (ICT) have profoundly transformed the ways in which individuals interact, collaborate, and share information, including in the health care sector (Abbott & Coenen, 2008). In line with global trends, health information technology services have become increasingly essential, particularly in the era of the Fourth Industrial Revolution (Industry 4.0), which presents both significant opportunities and complex challenges for health sector (Suyudi et al., 2025). Despite these advancements, health care technology innovation continues to face numerous obstacles, including pressures linked to demographic growth. Nonetheless, the integration of technological tools has enabled improvements in prevention, treatment, care delivery, and rehabilitation, making health services more efficient, effective,

and patient-centered (Utomo, Gultom, & Afriana, 2020).

All recent technological advancements have profound implications for Patient Confidentiality. Law professor Daniel J. Solove defines privacy as an individual's right to control the timing, manner, and context in which their personal information is shared (Labadie & Legner, 2023). In today's globalized and highly digitalized environment, Patient Confidentiality is essential for three key reasons: safeguarding security, protecting individual rights, and fostering trust. Individuals are far more likely to trust organizations that demonstrate a strong commitment to protecting their personal information (Alpiah et al., 2024).

Data protection is a legal requirement in Indonesia as stated in Article 28, paragraph (1) of the 1945 Constitution of the Republic of Indonesia. The Constitution guarantees that every individual has the right to be protected from harm, including threats to their person, family, honour, dignity, and property (Ardiansyah & Ardiana, 2023). Law Number 27 of 2022 on Personal Data Protection provides the primary legal framework governing the collection, use, storage, and safeguarding of personal data.

There were 124 reported data breach allegations handled by the Ministry of Communication and Information between 2019 and 2024. Of these, 111 cases involved the leakage of personal data (Ardiansyah & Ardiana, 2023). Personal health data, which includes information relating to an individual's medical history, current health condition, laboratory test results, prescription records, and other identifying health information, is particularly vulnerable to misuse (Sarastri, Saputro, & Hartini, 2021). Advances in technology have enabled medical records to be stored both physically and digitally, increasing accessibility and improving management. However, this ease of access also carries significant risks, including data breaches and the unauthorized use of sensitive health information.

Two of the four categories of health-related data identified by Deven McGraw and Kenneth D. Mandl are addressed in this article (McGraw & Mandl, 2021):

1. Health data generated by the healthcare system constitutes one of the two categories discussed in this article. Whenever a patient receives medical treatment, clinical personnel or medical equipment record information related to that encounter. This includes electronic medical records, medication lists, laboratory test results, radiographs, pathology images, and insurance claim data. Clinical data documents both the patient's medical history and current condition and is essential for determining appropriate treatment. Recording clinical information throughout a patient's life and enabling its exchange among healthcare providers are crucial for improving the quality and continuity of care. Because of its sensitive nature, the confidentiality of

clinical data is paramount. For this reason, most health-related legislation places strong emphasis on protecting the privacy and security of clinical information (Archer et al., 2011).

2. Health and fitness data generated for public use. This category of supplementary health data complements clinical data. It refers to information collected through applications or software used by individuals to manage their health independently. These tools, devices, and platforms provide consumers with insights into their daily health status and play an increasingly important role in self-management, particularly for individuals with chronic conditions (Alpay et al., 2009).

Table 1.
Summary of Clinical Data and Consumer Health Data

Data Aspects	Clinical Health Data (medical networks, healthcare experts, surgical tools)	Consumer Health Data (tangible electronic gadgets and wellness applications)
Recorded By	Medical treatment networks, healthcare experts, and surgical tools	Electronic gadgets (e.g., watches, bracelets), wellness applications
Data Details	Patients' names, ages, addresses, phone numbers, medical records, family medical records, symptoms, diagnoses, treatments, medications, and more	Personal information (e.g., name, ID, phone, address, job title, age, weight, height, pulse, respiration rate, blood pressure, glucose levels, activity history, dietary preferences, online consultations)
Data Characteristics	Passive data stored in the healthcare system, discrete, professionally managed, clinically oriented, with stronger privacy protection	Collected from diverse sources, ongoing standardization, high volume, more privacy concerns, and managed by multiple private service providers

Source: (Institute of Medicine (US) Roundtable on Value & Science-Driven Health Care, 2010) ; (Ivan, 2019)

As the healthcare industry continues to collect, store, and transmit increasing volumes of data, concerns about patient privacy have become more prominent (Meinert et al., 2018). Sensitive health information is particularly vulnerable to misuse and breaches, making its security a critical priority. The digitization of health records ranging from electronic medical records (EMRs) to data generated through wearable devices and mobile health applications has undoubtedly enhanced the efficiency, accessibility, and quality of healthcare services. However, this rapid digital transformation has also exposed patient information to greater risks of unauthorized access, improper use, and data leaks. Given the highly sensitive nature of health data, which often includes medical diagnoses, personal identifiers, and behavioral information, ensuring its protection is not only a technical necessity but also a legal and ethical obligation (Lestari et al., 2024).

Numerous legislative and regulatory

frameworks have been established worldwide to govern and protect medical data. Indonesia and the United Arab Emirates (UAE) are two countries that have made significant progress in developing regulations on the confidentiality and security of health information. In the UAE, the protection of patient privacy, the processing of health data, and the use of such data for evidence-based policymaking are primarily regulated by Federal Law No. 2 of 2019 concerning the Use of Information and Communication Technology in the Health Sector. Health Patient Confidentiality in the UAE is governed both by federal legislation and by the specific rules of special economic zones such as the Abu Dhabi Global Market and the Dubai International Financial Centre. These frameworks draw inspiration from international standards, including the EU's General Data Protection Regulation. The Dubai International Financial Centre Data Protection Law No. 5 of 2020 and the Abu Dhabi Global Market Data Protection Regulations 2021 impose strict requirements for the protection of personal data, including health information (Alhajaj & Moonesar, 2023).

Law 17 of 2023 on Health was enacted in Indonesia with a similar objective. This legislation regulates several aspects related to patient Patient Confidentiality within the Indonesian health system. Articles 114 and 116 emphasize the obligation to protect the confidentiality of patients' medical records. Indonesia also has additional sector-specific laws addressing this matter. For example, the Medical Practice Law Number 29 of 2004 (Utomo, Gultom, & Afriana, 2020), requires that all doctors, dentists, and heads of health service facilities create accurate medical records and maintain their confidentiality. In today's digital environment, individuals are increasingly integrated into digital systems, often at the cost of reduced control over their personal information and diminished data sovereignty (Eckhoff & Wagner, 2018).

Numerous countries have enacted legislation to ensure the confidentiality of patient information, recognizing its importance on a global scale. Although national approaches to personal data protection vary, several international and regional frameworks provide shared foundations for safeguarding privacy. By the end of 2019, 142 countries had adopted Patient Confidentiality laws, a significant increase from 62 countries in 2010 (Greenleaf & Cottier, 2020). Indonesia and the UAE are among the nations that acknowledge the necessity of protecting citizens' health information from misuse and preserving their fundamental rights. Comparing the legislative frameworks and health Patient Confidentiality regimes of these two countries therefore offers valuable insight into how each system operates, and allows us to identify the strengths and weaknesses of their respective regulatory models.

Individuals' rights over their personal data constitute a central element of modern Patient Confidentiality regulations (Wilona, Latifah, &

Purwadi, 2021). In the United Arab Emirates, regulations such as Federal Decree-Law No. 45 of 2021 on Personal Data Protection, along with the frameworks applied within the Dubai International Financial Centre and the Abu Dhabi Global Market, grant individuals the right to access, rectify, and erase their data. These rights ensure that individuals can exercise control over their personal information and pursue remedies in cases of misuse (Nair & Ibrahim, 2015). Indonesia provides similar protections, including the rights to access, correct, delete, and restrict the processing of personal data. These rights are intended to enhance individual autonomy and promote greater transparency regarding data use. However, the practical effectiveness of these protections remains heavily dependent on the consistency and rigor of law enforcement practices (Suari & Sarjana, 2023).

Compliance with data privacy legislation requires the involvement of enforcement authorities and the imposition of sanctions. In the United Arab Emirates, violations of Patient Confidentiality laws may result in strict administrative penalties. In Indonesia, individuals who infringe upon Patient Confidentiality rights may face both civil and criminal sanctions (Anggraeni, 2018). Ensuring compliance ultimately falls under the responsibility of the designated supervisory authorities in each jurisdiction. However, the central challenge remains achieving consistent and effective enforcement across the entire country.

Both nations must urgently strengthen the protection of patient health records against unauthorized access and data breaches. Comprehensive regulations clearly defining data responsibilities, processing limits, and accountability mechanisms are essential. As information and communication technologies continue to evolve rapidly, the issue of medical Patient Confidentiality has become a central topic in global legal and policy discussions (Ohoiwutun et al., 2024).

The governments of many countries have adopted regulations aimed at protecting the privacy of citizens' health information. In Indonesia, several legal instruments regulate the protection of health data, as noted by Pratama RA (2020). These include Law No. 11 of 2008 on Electronic Information and Transactions and Minister of Health Regulation No. 24 of 2020 concerning electronic medical records. Despite this regulatory framework, significant implementation challenges remain particularly the limited awareness and understanding of Patient Confidentiality obligations among the public and healthcare personnel (Hendra et al., 2021).

Both countries must take urgent steps to protect patient health records from unauthorized access and data breaches. Clear and comprehensive regulations defining data responsibilities and permissible uses are essential. As information and communication technologies rapidly evolve, health Patient Confidentiality has become a central issue in

international policy and legal discussions.

Globally, governments have enacted various rules to safeguard the confidentiality of citizens' health information. In Indonesia, several legal instruments regulate health data protection, including Law No. 11 of 2008 on Electronic Information and Transactions and Minister of Health Regulation No. 24 of 2020 on Electronic Medical Records. Despite this regulatory framework, significant challenges remain particularly the limited awareness and understanding of Patient Confidentiality obligations among both the public and healthcare professionals.

Heriyanto (2023) examined the legal frameworks and safeguards governing the privacy of patients' medical records in three Southeast Asian countries: Laos, Singapore, and Indonesia. His comparative study evaluates key components such as patients' rights, data security standards, consent mechanisms, cross-border data transfer regulations, and the roles of national data protection authorities. The findings reveal notable differences in the strength and effectiveness of the three systems. Singapore's Personal Data Protection Act stands out for its comprehensive approach, robust enforcement mechanisms, and mandatory data-breach reporting obligations. In contrast, although Laos and Indonesia have taken important steps toward protecting patient information, both countries still require significant improvements. These include clearer procedures for reporting data breaches and greater alignment with international data-protection standards. Persistent challenges identified across the region include limited resources, insufficient awareness and compliance among stakeholders, cybersecurity vulnerabilities, and obstacles related to cross-border data exchange (Iswandari & Hoque, 2022).

The UAE has also had its fair share of successes and failures in recent years when it comes to enforcing regulations protecting the privacy of patients' medical records. Health Patient Confidentiality is an important topic, an Sarabdeen, Moonesar, (2018) compared regulatory frameworks in the United Arab Emirates (UAE) to those of the EU and USA. They found that patient confidentiality remains far from meeting international standards. To improve Dubai's e-health regulatory framework, they proposed several areas for enhancement, particularly regarding patient confidentiality and the mechanisms required to ensure its effective protection (Sarabdeen & Moonesar, 2018).

Although many countries have made notable progress in protecting medical records, the literature indicates that significant challenges remain before robust and harmonized standards for Patient Confidentiality and security can be fully achieved. This underscores the importance of raising public awareness about health information privacy rights and empowering individuals to exercise greater control over their health data. Educational initiatives play a critical role in

improving public understanding of data security, consent, and individual rights related to the handling of personal health information.

There is limited regional and international literature directly comparing the privacy regulations governing medical records in the UAE and Indonesia. This gap highlights the need for a more systematic analysis of how these two countries regulate, implement, and enforce health data protection. By examining and contrasting their respective legal frameworks, this research seeks to deepen our understanding of the effectiveness of existing regulations and their practical application in different institutional contexts. To support this objective, a concise literature review was conducted to frame the discussion and situate both countries within the broader landscape of global health Patient Confidentiality initiatives.

Many studies have explored different dimensions of privacy and personal data protection, with several focusing on the legal frameworks and policy implementation in specific jurisdictions. For example, Simamora (2022) examines how Indonesia safeguards the privacy rights of COVID-19 patients, while research by Lintang and Triana (2021) reviews personal data protection within Indonesia's population administration system. In the UAE context, Alhajaj and Moonesar (2023) analyze public perceptions and the practical implementation of technological tools designed to protect personal data in Dubai. Furthermore, studies by Sarabdeen published in 2018 (Sarabdeen & Moonesar, 2018) and in 2025 (Sarabdeen & Ishak, 2025), provide comparative insights into data protection regulations and practices in the public and health sectors across Southeast Asia.

To shed new light on the topic, this study compares and contrasts the legal frameworks and medical Patient Confidentiality regulations of Indonesia and the United Arab Emirates (UAE). Its novelty lies in examining medical Patient Confidentiality through a dual-system perspective, assessing not only the statutory provisions but also the enforcement practices adopted in each country. Thus, the study goes beyond merely outlining existing regulations; it evaluates how both jurisdictions penalize and respond to violations of patient data confidentiality. While previous research has largely focused on single-country assessments or broad regional overviews without in-depth bilateral comparison, this study addresses that gap by offering a more nuanced and practical understanding of the strengths and weaknesses of each system.

This study seeks to answer two main research questions based on the discussion above:

(1) How do the legal frameworks and medical Patient Confidentiality regulations of Indonesia and the United Arab Emirates (UAE) compare?

(2) How do the penalties and enforcement mechanisms for breaches of medical Patient Confidentiality differ between Indonesia and the UAE?

B. RESEARCH METHODS

The normative legal research method is used in this study to evaluate and understand the rules, principles, and standards that operate within social, ethical, and legal frameworks. This method aims to determine what the law should prescribe by analyzing legal norms, doctrines, and principles contained in statutory regulations, legal dictionaries, and relevant literature.

It is appropriate for this research because it focuses on assessing the adequacy and consistency of legal provisions governing the protection of medical Patient Confidentiality. In addition, the study employs a comparative method to examine how these legal protections are enforced in both the United Arab Emirates and Indonesia.

The legal materials used consist of primary sources such as legislation, government regulations, and judicial decisions, as well as secondary sources including academic commentaries and scholarly articles. These sources are collected through document analysis and systematically compared to identify key differences and similarities in each country's regulatory and enforcement framework (Amiruddin & Asikin, 2012).

This study compares the first issue formulation concerning the enforcement of laws on medical Patient Confidentiality in the United Arab Emirates and Indonesia. It examines how both countries establish and implement the legal frameworks designed to protect patient privacy and ensure the confidentiality of medical records. The objective is to explore more deeply the extent of the state's obligation to safeguard the privacy rights of its citizens. Accordingly, this study analyzes the legal provisions governing medical data protection and identifies the legal consequences imposed on individuals or entities that violate these protections.

C. RESULTS AND DISCUSSION

1. UAE Legal Framework

The Federal Law No. 2 of 2019, also known as the Federal Law Concerning the Use of Information and Communication Technology in the Health Sector in the United Arab Emirates, represents a major advancement in regulating and protecting health data in the country. Prior to its enactment, the legal framework governing Patient Confidentiality and health information was fragmented across different sectors and jurisdictions. The law now requires healthcare providers, insurance companies, and other related entities to comply with strict rules governing the collection, processing, and transfer of health data. It stands as the first federal privacy law in the UAE specifically dedicated to the protection of health information.

The United Arab Emirates (UAE) approved Federal Decree-Law No. 45 of 2021 on Personal Data Protection on November 5, 2021. This legislation establishes a comprehensive framework governing the collection, processing, and use of personal data, with the primary

objective of safeguarding individuals' Patient Confidentiality. It serves as the UAE's federal-level data protection law and operates alongside other sector-specific regulations, ensuring a more coordinated approach to protecting personal information across different fields (UAE – Data Protection Overview, 2022).

The Federal Decree-Law requires all organizations that handle personal data to implement a comprehensive data protection strategy (Abouahmed, Kandeel, & Zakaria, 2024). This strategy must clearly outline the purposes of data collection, the methods of processing, and the restrictions on data use, ensuring that all personal data is handled lawfully. Personal information may only be obtained with the data subject's consent or under circumstances permitted by law, and it must be stored securely to prevent unauthorized access or disclosure. The regulation further specifies that only authorized individuals or entities may access personal data and solely for legitimate, predefined purposes. To highlight the key similarities and differences between the regulatory frameworks of the UAE and Indonesia, the following table provides a concise comparative overview. This summary also serves as a transition to the subsequent section, which examines how health data is processed in both jurisdictions.

Table 2.
Comparative Summary of Legal Frameworks Governing Medical Patient Confidentiality in the UAE and Indonesia

Aspects of Regulation	United Arab Emirates (UAE)	Indonesia
Legal Basis	Federal Law No. 2 of 2019; Federal Decree-Law No. 45/2021; Health Data Law (2023)	Law No. 27 of 2022 on Personal Data Protection; Law No. 17 of 2023 on Health
Scope of Protection	Covers personal health data in digital systems, including AI and electronic devices	Protects personal data, including health information, collected by healthcare institutions and platforms
Responsible Authority	UAE Data Office; Ministry of Health and Prevention	Ministry of Communication and Informatics (Kominfo); Ministry of Health
Sanctions for Violations	Administrative fines, suspension of licenses, criminal charges	Administrative, civil, and criminal sanctions; fines and imprisonment
Implementation Challenges	Need for harmonization across emirates and coordination between federal and local authorities.	Weak institutional coordination, limited resources, and public awareness
Technological Readiness	Advanced digital health infrastructure; integrated national health data strategy	Fragmented digital systems; limited interoperability among health data systems

Source: Author's own research (2025)

If individuals suspect that their data has been mishandled or improperly used, they may file a complaint with the relevant authorities. To prevent future violations, the law imposes penalties that correspond to the seriousness of the offense. Article 7(1) of the UAE Personal Data Protection Law requires personal data to be protected against leakage, damage, or unauthorized access. It also obliges data controllers to ensure that personal data is stored

securely and accessed only by authorized persons. Article 8(2) strengthens this obligation by emphasizing that only individuals who are legally permitted may process personal data. As a result, access rights must be clearly defined, including information on how personal data is used and the mechanisms through which it is accessed.

Additionally, the Dubai Health Authority oversees and enforces health standards in both public and private healthcare institutions in Dubai. This strategy is a key component of a well-run healthcare system, and it reflects the Dubai Health Authority's dedication to health preservation and improvement. To ensure compliance with the processes and regulations outlined in Federal Law No. 2 of 2019 and Federal Law No. 45 of 2021, the Dubai Health Authority has designated a Data Protection Officer to oversee matters about the security of patient records. The Data Protection Officer's primary responsibility at the Dubai Health Authority is to handle complaints of data leaks and implement measures to rectify the situation.

The Personal Data Protection Law of the United Arab Emirates (UAE) incorporates several provisions and guidelines from the General Data Protection Regulation (GDPR). The General Data Protection Regulation only permits the collection of personal data with the consent of the data subject or as mandated by law. A regulation in the United Arab Emirates stipulates, among other things, that obtaining personal information requires the consent of the data subject or specific legal reasons. Article 4 paragraphs (1) and (2) of Federal Decree-Law No. 45 of 2021 outline this regulation. Accurate and thorough documentation of data collection procedures, including information on the data's intended use, is required when collecting personally identifiable information (GDPR.EU, 2018).

In light of the complexity of Patient Confidentiality and security in the digital age, these standards constitute a substantial advance. Federal Law No. 2 of 2019 and Federal Decree-Law No. 45 of 2021 demonstrate a firm dedication to safeguarding personal information and public health in the United Arab Emirates, while international pressures like the General Data Protection Regulation offer further incentive to enhance data protection standards generally.

2. UAE Medical Privacy Data Processing

The proliferation of data from mobile networks, computer systems, health apps, and electronic medical records is fueling the expansion of patient data and information for health care. These systems are becoming more comprehensive. Kumar N & Manjula stressed that hospitals and other medical centers produce vast amounts of data about patients, drugs, treatments, illnesses, studies, and related topics (Kumar N & Manjula, 2014). Electronic medical records (EMR) are a digital platform that may be used to manage health data. Patients' vital records are abundant on this platform. From patient demographics to test findings, imaging, and radiology, it's all recorded in the EMR. The

symptoms and development of illnesses may be better understood with the use of data stored in the EMR (Effoe et al., 2016). Results from the Lifestyle Intervention for Treatment of Diabetes study demonstrate the effective use of electronic health data in clinical trial recruitment. EMR can also address issues related to disease progression, comorbidities, and mortality (Paxton, Niculescu-Mizil, & Saria, 2013). Electronic health records, household sensors, and wearable technology are just a few places you may find this data (Laney, 2001).

Big data in health refers to data sets that are too big for traditional computer algorithms to analyze (Wang et al., 2016). Sorted according to its structure, big data may be either fully or partially organized. First, there is a specific format for storing, retrieving, and processing structured data. Unlike the previously mentioned layout of structured data, unstructured data lacks a clear structure, resulting in a distinct and dedicated type of data that is easy to obtain and understand. According to Wu and Lin, there are a lot of processing issues with this data type when it comes to retrieving meaningful information (Wu & Lin, 2018). Some examples of processing resource limits include problems with data, language, identifying relationships, and technology (Adnan & Akbar, 2019). The existing approaches to data extraction from diverse, unstructured, large data sets have significant drawbacks. We use a holistic approach, using suitable simulated healthcare datasets, to assess the efficiency and resilience of different data (Gao et al., 2017), and 3) a system that collects patient information from multiple databases. The process of linking devices and gathering data begins here. This is critical when optimizing multiple databases (Zhang & Hansen, 2007).

Social and legal technicalities may present obstacles to the collection of health big data. These social and legal issues may arise due to concerns about data ownership, privacy, identification, and health governance (Mittelstadt & Floridi, 2016). As health information becomes increasingly digitized and interconnected, addressing these concerns through clear legal frameworks and ethical standards is essential to ensure trust and compliance within health data ecosystems.

Article 12 of the Federal Law mandates that the UAE's health data adhere to ministerial regulations, requiring coordination with the Minister of Health. This is consistent with Article 13 of the Federal Law, which establishes obligations for the storage of healthcare data and information both within and outside the UAE. Health data or information may not be stored, processed, created, or transmitted outside the UAE about health services provided in the UAE, except through a resolution issued in support of health care data or information processors in coordination with the Ministry, as per Article 13 (Coorevits et al., 2013). This article has sparked significant debate and controversy due to the fact that numerous organizations process health data

and information outside of the UAE. Nevertheless, the UAE's healthcare data and information management industry sectors are relieved by the exceptions and exemptions to Article 13 provided by Article 12 of Ministerial Decree No. 51 of 2021. The following exceptions are enumerated in Article 2 of the Decree: (1) Data utilized in scientific research; (2) Data required by international organizations that collaborate with the UAE government; (3) Data concerning samples sent to laboratories outside the UAE; (4) Data required by insurance companies and claims administration agencies; (5) Data collected by basic medical devices and equipment; (6) Data utilized in the provision of online health services; and (7) Data concerned with patient diagnosis, treatment, or prevention.

In addition, Resolution No. 40 of 2019 pertains to the implementation of medical liability law in the UAE and contains provisions concerning the provision of "Remote Health Services." Article 2.1(f) of the resolution mandates the existence of a server within the country to display and store information and backup (Tithecott & Jhala, 2019), These include the following: (1) Server Requirements: These provisions mandate that remote health service providers maintain servers within the United Arab Emirates' territorial jurisdiction. (2) Information Storage and Security: These requirements are designed to guarantee the secure storage of sensitive health information. Safe and in compliance with current laws and regulations, (3) Backup Requirements: This provision also underscores the significance of having a backup system in place to prepare for data loss or system failure. (4) Compliance and Supervision: This regulation mandates the establishment of servers and backups within the country to facilitate regulatory oversight and compliance monitoring by authorities.

3. Indonesian Legal Framework

One of the primary concepts of the 1945 Constitution of the Unitary State of the Republic of Indonesia is that the state is responsible for the protection of the entire Indonesian nation and all Indonesian blood by ensuring social justice for all Indonesians, as determined by unity. The state's protection of citizens' property rights illustrates this concept. According to Article 28H, paragraph 4, of the 1945 Constitution of the Unitary State of the Republic of Indonesia, every individual is entitled to private property rights, which may not be arbitrarily seized by any individual (Taufiqurrohman et al., 2024).

We are all aware that property rights are regulated by Civil Law (Burgerlijk Wetboek). Despite Indonesia's independence, the 1945 Constitution of the Unitary State of the Republic of Indonesia retains the validity of the law until a new law replaces it. Of course, Article 570 of the Burgerlijk Wetboek regulates the authority and restrictions for property rights holders. These provisions also apply to the proprietorship of medical records. We understand that neglecting the obligation to protect information in patient

medical records violates both the patient's right to privacy and their property rights. Furthermore, accessing and using the contents of medical records without the patient's consent should not violate their property rights (Daeng et al., 2023). As a result, the confidentiality of medical data in Indonesia is critical for safeguarding patient health information.

Law Number 36 of 2009 concerning health regulates the privacy of patient health data, underscoring the importance of medical record confidentiality. According to Article 46, health service facilities are required to maintain the confidentiality of medical records. Authorized parties should have access to personal health information, and patient consent is required for its use for any other purpose. Article 55 states that every individual has the right to access confidential health information that a health service provider stores. This underscores the significance of controlled and secure access to health information. Additionally, Article 52 governs the patient's entitlement to receive health information that is transparent, truthful, and comprehensible. The objective of this legal framework is to enhance the quality of health services and safeguard patients' privacy rights.

The implementation of this law in society continues to encounter a variety of obstacles. Many health facilities, particularly those located in remote locations, struggle to maintain the confidentiality of medical records due to inadequate technology and human resources. Furthermore, the public does not fully understand their rights regarding the privacy of health data. Health professionals continue to misuse information, which constitutes a violation of medical Patient Confidentiality. Nevertheless, the government is making ongoing efforts to address this challenge by enhancing infrastructure and educating the public (Bunga, 2015)

The government issued Minister of Health Regulation Number 269/MENKES/PER/III/2008 to regulate medical records. A health care provider maintains a medical record, which is a compilation of medical information about a patient. This information encompasses the patient's medical history, diagnosis, examination results, medication prescriptions, and other pertinent records regarding the patient's care. Coordinating care among multiple health care providers and documenting and monitoring the provided care is crucial.

Article 10 of the Indonesian Minister of Health Regulation No. 269/Menkes/Per/III/2008 on Medical Records stipulates strict confidentiality regarding patients' identity, diagnosis, medical history, and treatment. This information must be protected by healthcare professionals and facility managers. However, disclosure may be permitted under specific conditions, such as: (a) for the benefit of the patient’s health; (b) at the request of law enforcement with a court order; (c) based on the patient’s request or consent; (d) at the request of other institutions under statutory authority; or (e) for research or educational purposes, provided

the patient's identity is not revealed. In addition, all requests for medical records must be submitted in writing to the head of the health facility.

Article 10 paragraphs (1), (2), and (3) stipulate that access to or disclosure of medical records to other parties requires the patient's consent, except for specific purposes like law enforcement or court requests. This aims to ensure that patient medical information remains confidential and protected from unauthorized access. Health workers are also required to provide adequate explanations to patients regarding the purpose and benefits of collecting medical data (Sanjoyo, 2007)

As stated in Article 13, this Minister of Health Regulation requires standard operating procedures to protect the confidentiality of medical records. There will be both administrative and technological safeguards in place to stop the disclosure or abuse of sensitive data. The goal of implementing this rule is to ensure that patients' medical data remains private, giving them peace of mind when seeking healthcare.

According to Article 13 of the Minister of Health Regulation No. 269 of 2008 on Medical Records, the use of medical records is limited to specific purposes such as patient healthcare, law enforcement proceedings, professional discipline, research and education, cost regulation, and health statistics. If the use of medical records involves identifying patient data, especially for law enforcement or personal request purposes, explicit written consent from the patient or their legal heirs must be obtained. However, patient consent is not required when medical records are used for state interests in the context of research and education, provided that confidentiality is still maintained.

Article 13 of Minister of Health Regulation Number 269/MENKES/PER/III/2008 governs the management of medical records, including the production, storage, and use of patient health information. In line with recognized medical ethical principles, its execution highlights the need to keep data secret. Compliance with such rules, as Indriyati pointed out, helps lessen the likelihood of privacy breaches and boosts patients' faith in the healthcare system. Within this framework, the execution of this article also urges healthcare providers to guarantee that only authorized individuals with valid medical needs may access patient information (Indriyajati, Jawa, & Utomo, 2023).

The goal of Indonesia's Law Number 44 of 2009 on Hospitals is to ensure that all patients' medical records remain private by regulating several areas of hospital administration, including the protection of patient data. Article 32I guarantees the right to privacy and secrecy for all medical records and information about a patient's illness. Article 44, Paragraph 1, states that "Hospitals can refuse to disclose any information to the public relating to medical secrets." This provision guarantees the legal protection of hospitals. Article 44, Paragraph 1 of Law Number

44 of 2009, which regulates hospitals, protects hospitals legally from the public disclosure of sensitive medical information. Information about the patient, their diagnosis, and the care they received may be considered medical secrets, and the hospital may choose not to divulge it. Doing so prevents unauthorized parties from gaining access to or misusing, patients' medical records (Yustina, 2012).

The government enacted Law 17 of 2023 in the health field to enhance the standard of health services, safeguard the public, and regulate the powers and duties of health professionals. Changes in health care technology and the lessons learned during the COVID-19 epidemic prompted a reorganization of Indonesia's healthcare system, which in turn led to the passage of this legislation. We will build this reform around six pillars: primary care, referral services, health security, financing, human resources, and health technology, all aimed at promoting a robust and healthy Indonesian society. We anticipate that this law will also provide legal protections for health care providers. This health law has the potential to improve the health of the Indonesian people by ensuring that they have access to top-notch healthcare (Kesuma, 2023).

Law Number 17 of 2023 contains patient Patient Confidentiality rights, as Article 177 states that:

a. Every Health Service Facility must keep the patient's personal health secrets.
b. Health Service Facilities may refuse to disclose any information to the public relating to the patient's health secrets, except based on the provisions as provided in Article 4 paragraph (4).

Furthermore, Article 296 of Law Number 17 of 2023 states that patient medical records must be maintained and kept confidential by specific obligations. Paragraph (5) explains these responsibilities, stating: *"Every medical worker and health worker who provides individual health services is required to keep a medical record. In the event, as intended in paragraph (1), it is carried out at a Health Service Facility other than an independent practice place, the maintenance of medical records is the responsibility of the Health Service Facility. Medical records as intended in paragraph (1) must be completed immediately after the patient has finished receiving health services. Each medical record entry must contain the name, time, and signature of the Medical Personnel or Health Personnel providing the service or action. Medical records as intended in paragraph (3) must be kept and kept confidential by Medical Personnel, Health Personnel, and leaders of Health Service Facilities."*

Article 301 paragraph (7) of Law No. 17 of 2023 addresses patient health confidentiality and constitutes the final provision related to health Patient Confidentiality. It states: *"Every Medical Personnel and Health Personnel in carrying out Health Services is obliged to keep the patient's*

personal health secrets. Disclosure of the patient's personal health secrets as intended in paragraph (1) can be carried out for certain purposes as intended in Article 4 paragraph (4)." This regulation reinforces the duty of confidentiality while recognizing that exceptions are permissible under clearly defined legal parameters.

4. Indonesian Medical Privacy Data Processing

Hospital management information systems and related technology have improved efficiency in the storage, processing, and interchange of medical data (Rahmouni, Essefi, & Ladeb, 2019). In order to better manage their data and service operations, hospitals might benefit from using a Hospital Management Information System. A hospital's management information system (HIS) is a computer program that streamlines and unifies the flow of all business operations related to health services. It does this via an interconnected web of reporting, coordination, and administrative procedures that allow for the efficient and correct retrieval of data (Muntari et al., 2020).

The Minister of Health Regulation No. 82 of 2013 establishes the guidelines for the application of these regulations in Indonesia. Every healthcare facility is mandated to establish a hospital management information system according to this rule. Hospital Management Information Systems must meet the standards and requirements of the Health Ministry and National Standardization Agency, along with documentation and evidence certification from independent institutions like ISO or HIMSS. Additionally, these systems must be able to provide technical support and maintenance throughout the contract period. A business license from the Ministry of Communication and Information is also required (Akbar, 2018).

There are many important ways in which hospitals and patients may benefit from hospital management information systems. In order to better manage patient data, streamline administrative procedures, and improve the efficiency of health services, hospitals may use hospital management information systems. Healthcare facilities can reduce patient wait times and streamline administrative tasks by integrating various systems, including insurance and payment processing. Protecting patient privacy and adhering to privacy standards are two of hospital management information systems' most important functions. Medical facilities have a responsibility to safeguard their patients' personal information by implementing measures to prevent unauthorized access, use, disclosure, or alteration (Situmorang, 2022).

A number of challenges have impeded the rollout of HMIS in Indonesian hospitals. Because they do not have thorough IT management, several hospitals still have trouble deploying HMIS. The internal development of a hospital management information system requires a substantial investment of time, energy, and

money. Therefore, it is prudent to select a provider who offers a hospital management information system. The Indonesian Hospital Management Information System has reported multiple instances of data breaches. The Arifin Achmad Regional General Hospital in Riau Province, for example, has seen a significant improvement in the efficiency and effectiveness of its operations across all departments after implementing a hospital management information system. However, hospitals must exercise extreme caution while handling patient data in order to prevent data breaches when using a hospital management information system. Although HMIS has the potential to increase hospital efficiency, improperly implemented systems increase the danger of data breaches (Rifly, 2022).

5. Sanctions and Enforcement for Violations of Medical Patient Confidentiality Compared Between the United Arab Emirates (UAE) and Indonesia

The UAE and Indonesia both prioritize personal data security by enforcing penalties and sanctions against breaches of patients' medical Patient Confidentiality. When people break the laws or norms that society has set up, the system responds by imposing sanctions. Sanctions, in Rahayu's view, are a means of disciplining wrongdoers and discouraging repeat offenses. Depending on the seriousness of the offense, the offender may be subject to fines, jail time, license suspension, or other punishments (Rahayu, 2017).

There have been problems with patient data leaking lately, even though the aforementioned law regulates the secrecy of patient health data. One of the factors that might contribute to breaches involving medical data leakage is a lack of stringent oversight and control over medical data. Another cause of data leakage infractions is a lack of understanding of the rules and regulations in place (Susanto, 2019).

Health data security breaches in the United Arab Emirates (UAE) are subject to penalties and law enforcement action according to a number of pieces of legislation, the most recent of which is Federal Law No. 2 of 2019, which lays out the rules in detail. Articles 25 and 26 of this Law, among others, stipulate that any breach of the rules governing the gathering, processing, or transmission of health data may result in an administrative punishment of up to a specified amount. More significant infractions may trigger further legal action, including criminal prosecution. Article 27 may enforce administrative penalties for infractions of this legislation.

A substantial monetary punishment is one possible administrative consequence; the exact amount may vary according to the severity of the breach and its effect on the security of protected health information. This law empowers authorities to investigate incidents, gather evidence, and take appropriate action to prevent or remediate health data breaches. The penalties for violating this

legislation, as stated in Article 28, might include the suspension, revocation, or restriction of licenses or permits given to companies engaged in health data management, as well as the temporary or permanent termination of such permissions or licenses (van Velthoven et al., 2016).

The purpose of these regulations is to protect individuals' privacy and lessen the likelihood of misuse or unauthorized access to sensitive information by ensuring that all parties engaged in the acquisition, processing, or storage of health data in the UAE adhere to stringent standards in the protection of personal data, including health data. Yes, this. By passing Federal Law No. 2 of 2019, the United Arab Emirates reaffirms its will to tackle the modern data security crisis head-on by implementing robust measures to safeguard all health records.

Additionally, Federal Decree-Law No. 45 of 2021 pertaining to Personal Data Protection regulates penalties and the implementation of laws pertaining to the protection of health data. Article 21 of Federal Decree-Law No. 45 of 2021, which pertains to personal data protection, emphasizes administrative penalties for data protection law infractions. This article says that if you break the rules in Federal Decree-Law No. 45 of 2021 about Personal Data Protection, you can be fined, given written warnings, lose your permission to process personal data, have data processing centers closed temporarily or permanently, or be blocked from accessing system information temporarily or permanently. Administrative penalties may be as high as fifty million UAE dirhams (about thirteen and a half million dollars) or five percent of the offending entity's total yearly turnover. It is believed that these penalties will serve as a powerful disincentive for businesses and other organizations to adhere to the requirements of Federal Decree-Law No. 45 of 2021 on the careful management and protection of personal data, particularly health records.

Regarding law enforcement, Federal Decree-Law No. 45 of 2021 gives the Data Protection Committee the authority to investigate suspected violations, collect evidence, and take action by applicable legal provisions. This committee has the authority to order the violating company or organization to correct the violation, or, in the case of a serious violation, to refer the violation to court for further resolution by applicable criminal or civil laws in the UAE (Alostad, Steinke, & Schafheutle, 2018).

Even in Indonesia, there have been violations of medical Patient Confidentiality rules. According to Cyber Security Researcher Teguh Aprianto, the Data Inspection Team plans to file a lawsuit against the party responsible for the unauthorized disclosure of 279 million patient records from Indonesia's Social Security Administration for Health. There are strong suspicions of data breaches involving sensitive information such as Social Security Administration participant card numbers, office codes, family

details, health insurance dependents, and insurance payment statuses, according to Dedy Permadani (DA, 2021). In light of this breach, the state must take measures to secure the personal health information of its citizens and bring those responsible to justice

Law Number 36 of 2009 Concerning Health mandates that medical professionals (doctors, nurses, and hospitals) maintain the privacy of patient information and refrain from disclosing it to any other party without specific legal authorization. So, it's obvious that those who breach patient privacy by making their information public have broken the law.

Legislation, specifically Number 36 of 2009 concerning health, expressly prohibits careless individuals from disclosing patients' personal information, as stated in Article 57 paragraph (1) of the Constitution. As stated by health care professionals, often known as health workers, every individual has the right to access information about their health status. Everyone who commits themselves to health care, has formal education in the field, and, in the case of certain occupations, needs formal authorization to practice what they preach, is considered a health worker in this article.

As previously mentioned, the disclosure of patient personal data, specifically the patient's identity and health status, to third parties who violate the regulations outlined in Article 57 paragraph (2) of Law Number 36 of 2009 about health constitutes a violation of the law and warrants accountability. It follows that every individual has the right to seek redress for damages caused by the publication of health information, as stated in paragraph one of Article 58.

Similarly, Article 48, paragraph 1, of the Constitution of 2004 (Regarding Medical Practice) states that all dentists and doctors are required to maintain the confidentiality of any information they learn while treating patients, including but not limited to any findings made during treatment and documented in the patient's medical record. Private and protected patient medical records.

Article 38, paragraph 1, of Law Number 44 of 2009 concerning hospitals emphasizes the legal basis governing the confidentiality of patient information in Indonesia and states that not only doctors and dentists but also hospitals are required to maintain medical secrets. According to this article, all healthcare facilities are required to keep patient records private. This category includes everything required for medical care, including personal details, medical history, test results, and diagnosis. The purpose of implementing Article 38, paragraph (1), is to safeguard patients' right to privacy and prevent abuse or unauthorized access to sensitive information. As a result of this regulation, healthcare facilities must establish and adhere to stringent protocols for patient data management, including secure storage, appropriate access, and use of data in line with clinical requirements. The overarching goal is to adequately safeguard

patients' private rights by relevant legal concepts and medical ethics, while also preserving public trust in health services.

Law No. 36 of 2009 on Health, which deals with law enforcement matters, does not specify sanctions for violations of Article 57. However, other laws govern punishments; for example, Law 29 of 2004 governs medical practice. Article 51, Letter C of the Medical Practice Law, addressing the safeguarding of personal information, asserts the following:

> *"A doctor or dentist in carrying out medical practice must keep everything he knows about a patient confidential, even after the patient dies."*

If there is a violation of the above article, there will be legal consequences, as regulated in Article 79, letter c of Law Number 29 of 2004 concerning Medical Practice, the article states that:

> *"Sentenced with imprisonment for a maximum of 1 (or) year or a fine of a maximum of Rp. 50,000,000.00 (fifty million rupiah), every doctor or dentist who: deliberately does not fulfill the obligations as intended in article 51 letter a, letter b, letter c, letter d, or letter e."*

This confidential data can also apply to parties or individuals because of their position as regulated by the Criminal Code. Article 322, paragraph (1) of the Criminal Code states that:

> *"Anyone who deliberately discloses a secret which, according to his position or occupation, whether current or previous, is required to keep it, shall be punished by imprisonment for a maximum of nine months or a fine of up to Rp. 9,000."*

This law combines the provisions of the Criminal Code and the Constitution for Medical Practice to penalize individuals or entities that violate patient privacy by disclosing their medical records or other personal information. This includes medical professionals, hospitals, and other service providers in the health industry. Moreover, we can classify the reaffirmations into the following categories: The Constitution No. 19 of 2016 pertains to Top Amendments, while Constitution No. 11 of 2008 addresses Electronic Information and Transactions. As stated in the first paragraph of Article 26,

> *"Unless otherwise determined by statutory regulations, the use of any information via electronic media that concerns a person's data must be carried out with the consent of the person concerned."*

Articles 27–37 also prohibit activities without rights and the intentional misuse of electronic information that could harm others, in addition to paragraph (1) of Article 26. According to Article 46, paragraph (2), the penalties for a violation can be as high as 7 years in prison and a fine of up to 700,000,000 Rp. On the other hand, if it is proven that a third party has violated the misuse of personal data, met the criminal elements of that offense, and caused loss as a result, that person can be punished with up to 12 years in prison and/or a fine of up to 12,000,000 Rp. A person is threatened with a maximum fine

of Rp. 1,000,000,000 and/or imprisonment for a maximum of 6 years in Article 45A paragraph (1) if, intentionally and without authorization, they spread hoaxes or false news and mislead consumers, causing losses in electronic transactions as intended in Article 28 paragraph (1).

Furthermore, the Civil Code also regulates unlawful acts that harm other people, namely in Articles 1365, 1366, and 1367, including as following:

Article 1365;

> *"Every unlawful act that causes harm to another person requires the person whose fault it was to cause the loss to compensate for the loss.*

Article 1366;

> *"Every person is responsible not only for losses caused by his actions, but also for losses caused by negligence or lack of care."*

Article 1367;

> *"A person is not only responsible for losses caused by his actions, but also for losses caused by the actions of people who are his dependents or caused by goods under his control."*

In light of the above, it is easy to see how Article 1365 of the Civil Code lays forth the responsibilities that third parties have when they engage in illegal activities. Furthermore, Article 1366 of the Civil Code stipulates that an individual bears liability for any harm they inflict upon another, particularly in instances of carelessness or ignorance. A person's obligation, as stated in Article 1367 of the Civil Code, extends to losses inflicted by others who are dependent on him or who are under his supervision. The three articles that make up the Civil Code make it clear that when an individual or their dependents suffer financial harm as a result of another's illegal behavior, the Civil Law Act specifies how this harm might manifest.

6. Comparison of UAE and Indonesia Health Data Laws

The health data protection legislation in the UAE and Indonesia places an emphasis on the need for collecting and recording personal data in a legitimate, fair, and transparent way to ensure legitimacy, justice, and transparency. These commonalities highlight the significance of adhering to ethical and legal norms while dealing with personal data. However, as stated explicitly in Federal Decree-Law No. 45 of 2021, the United Arab Emirates provides more detailed instructions on this concept. The Federal Decree-Law No. 45 of 2021 highlights the significance of explicitly defining permission as the foundation of legitimate data processing procedures, along with the ideals of accountability and openness. Particular to the United Arab Emirates is the fact that local law protects individuals' privacy by granting them certain rights, such as the ability to see and amend their data. This improves patient protection and ensures appropriate and transparent handling of their data (Weber, Zhang, & Wu, 2020).

These two state statutes recognize the importance of limiting data usage, ensuring the relevance of personal data, and providing users with restricted access. This regulatory approach aligns with protecting individuals' privacy and security. To safeguard data against illegal or unauthorized processing, accidental loss, destruction, or damage, and to adopt suitable technological and organizational safeguards, the rule mandates their implementation.

By Law no. 45 of 2021, those entrusted with the care of patients' personal information must provide evidence of patients' permission before dealing with such information. Data user officers must be able to provide evidence of the patient's permission, as stated in Article 6's first point. This is by paragraph (2) of Article 10 of Minister of Health Regulation Number 269/MENKES/PER/III/2008. This shows that they are serious about safeguarding people's data rights and that they are committed to data protection standards that are known across the world. Both the UAE's and Indonesia's data privacy regulations have room for improvement, however (Abouahmed, Kandeel, & Zakaria, 2024). Clarifying the requirements and methods for gaining and withdrawing permission clearly and precisely is necessary to further expand the notion of patient consent for data users. Judicial oversight is necessary to protect the patient's (data owner's) rights and interests, even when data users have permission to access (El-Gheriani & Hashish, 2023)

The United Arab Emirates has rules that are more stringently enforced and have quantifiable penalties for managing medical Patient Confidentiality. Authorities like the Data Protection Officer at the Dubai Health Authority directly engage in effective legal enforcement against abuses of medical Patient Confidentiality. The UAE Data Office is an independent body with the power to investigate violations of data protection laws, levy fines on violating businesses, and enforce rules in order to guarantee the efficient implementation and enforcement of data protection legislation in the UAE. Ensuring compliance with data protection legislation and preserving personal data (Ghandour & Woodford, 2019)

In the meantime, there are regulations in place to safeguard medical data and ensure their consistent enforcement in Indonesia, but these rules are not always easy to implement. Enforcement often encounters practical barriers, such as limited public awareness, insufficient institutional coordination, and a lack of trained personnel within law enforcement and health institutions. Although there is less stringent law enforcement compared to the UAE, Indonesia provides a variety of legal sanctions for breaches of medical Patient Confidentiality. These penalties are more diverse and may include both administrative and criminal fines, depending on the severity and intent of the violation.

There is a better-organized system in place to handle medical Patient Confidentiality in the

UAE, with penalties for infractions that are both obvious and difficult to ignore. Indonesia has established laws to address breaches of patients' personal health information, but consistent enforcement of these laws is crucial for effective protection of patients' medical records.

The table below compares the statutory rules pertaining to health data protection in the UAE and Indonesia. The UAE enforces a more systematic and enforceable framework with well delineated punishments, whereas Indonesia has instituted pertinent legal requirements but need persistent enforcement to guarantee the proper safeguarding of patients' medical information.

Table 3.
Comparison Between Health Data Protection in the UAE and Indonesia

Aspect	UAE	Indonesia
Patient Consent	By law, patients' permission for data handling is required (Article 6 of Law No. 45 of 2021).	Patient agreement is required for access to health records, according to Article 10 paragraph (2) of Ministerial Regulation No. 269/MENKES/PER/III/2008.
Rights of access and correction of data by patients	Patients have the right to view and rectify their personal information.	Patients have the right to access and request correction or deletion of their data under Article 16 of Law No. 27 of 2022 on Personal Data Protection.
Oversight and enforcement	*The Data Office, Dubai Health Authority, United Arab Emirates.*	There is no established, distinct autonomous body.
Penalty	Federal Law No. 2 of 2019 contains Title 25, Article 26, Article 27, and Article 28. The penalties outlined in Federal Decree-Law 45 of 2021 also include: Administrative sanctions may reach up to fifty million United Emirates Dirhams (13,600,000 USD), or 220,861,487,398.4 IDR, or five percent of the offending agency's total revenue.	The maximum penalties are a fine of IDR 50,000,000 or a jail term of 1 year, as stated in Article 79, Letter C, of Law Number 29 of 2004 governing medical practice.

Source: (United Arab Emirates, 2019); (United Arab Emirates, 2021); (DPD PORMIKI DKI Jakarta, 2025); (Database Peraturan JDIH BPK, 2025a); (Database Peraturan JDIH BPK, 2025b)

While both the UAE and Indonesia take precautions to secure citizens' personal health information, there are also key distinctions. The United Arab Emirates has issued more specific instructions in Federal Decree-Law No. 45 of 2021, although both nations stress the need to

follow ethical and legal norms while dealing with personal data. The UAE enforces its rules more stringently and places a greater emphasis on the protection of medical data by the proper authorities. One of the UAE's autonomous regulatory bodies is the UAE Data Office, which punishes those who violate patients' right to privacy when it comes to their medical records. However, additional efforts are necessary to guarantee the consistent enforcement of the legislation and the adequate legal framework in Indonesia to address breaches of medical data privacy (Adonara, Ohoiwutun, & Taniady, 2025). However, legal provisions such as Law No. 27 of 2022 on Personal Data Protection and Law No. 29 of 2004 on Medical Practice not only regulate penalties for violations but also provide the foundational legal framework for safeguarding patient data autonomy and privacy. Despite their existence, consistent enforcement and the security of medical data remain areas where practical implementation continues to face significant challenges.

D. CONCLUSION

The comparative study of medical data protection laws in the United Arab Emirates (UAE) and Indonesia reveals significant disparities in legal enforcement, institutional frameworks, and normative clarity. In the UAE, the legal foundation for health Patient Confidentiality is robust, grounded in Federal Law No. 2 of 2019 and Federal Decree-Law No. 45 of 2021, with enforcement overseen by an autonomous body, the Dubai Health Authority. These statutes provide clear sanctions, including substantial administrative fines and criminal liability against violations, reflecting the state's firm commitment to data protection.

Conversely, while Indonesia has enacted multiple legal instruments, including Law No. 29 of 2004 on Medical Practice, Minister of Health Regulation No. 269/MENKES/PER/III/2008, and Law No. 27 of 2022 on Personal Data Protection, enforcement remains fragmented. There is no dedicated autonomous oversight institution, and regional disparities persist due to inconsistent implementation and weak institutional coordination. Moreover, the normative gap surrounding patients' right to access and rectify their medical data poses a challenge, even though Article 16 of Law No. 27 of 2022 technically recognizes such rights.

These findings suggest that Indonesia must improve regulatory clarity, establish an independent oversight body, and harmonize overlapping laws to ensure effective and consistent enforcement. Strengthening legal certainty and institutional capacity is crucial to safeguarding patients' rights and privacy, especially in an era of increasing digitalization of health services. Future research could focus on evaluating how these frameworks operate in practice, particularly in regions with limited infrastructure and administrative resources.

REFERENCES

JOURNALS

Abbott, P. A., & Coenen, A. (2008). Globalization and advances in information and communication technologies: The impact on nursing and health. *Nursing Outlook*, *56*(5),238–246. https://doi.org/10.1016/j.outlook.2008.06.009

Abouahmed, A., Kandeel, M. E., & Zakaria, A. (2024). Personal data protection in the United Arab Emirates and the European Union regulations. *Journal of Governance and Regulation,13*(1),195-202. https://doi.org/10.22495/jgrv13i1art17.

Adnan, K., & Akbar, R. (2019). Limitations of information extraction methods and techniques for heterogeneous unstructured big data. *International Journal of Engineering Business Management, 11*. https://doi.org/10.1177/1847979019890771

Adonara, F. F., Ohoiwutun, Y. A. T., & Taniady, V. (2025). The Application of the Res Ipsa Loquitur Doctrine as a Principle of Evidence in Medical Malpractice. *Jurnal Pembangunan Hukum Indonesia*,*7*(3),358–376. https://doi.org/10.14710/jphi.v7i3.179-197

Akbar, A. (2018). Design of information system of medical record web based inpatient public hospital in South Solo. *Jurnal Rekam Medic,1*(1),1–9. https://doi.org/10.33085/jrm.v1i1.3957

Alhajaj, K. E., & Moonesar, I. A. (2023). The power of big data mining to improve the health care system in the United Arab Emirates. *Journal of Big Data, 10*(12). https://doi.org/10.1186/s40537-022-00681-5

Alostad, A. H., Steinke, D. T., & Schafheutle, E. I. (2018). International comparison of five herbal medicine registration systems to inform regulation development: United Kingdom, Germany, United States of America, United Arab Emirates and Kingdom of Bahrain. *Pharmaceutical Medicine,32*(1),39–49. https://doi.org/10.1007/s40290-018-0223-0

Alpay, L., Verhoef, J., Xie, B., Te'eni, D., & Zwetsloot-Schonk, J. H. M. (2009). Current challenge in consumer health informatics: Bridging the gap between access to information and information understanding. *Biomedical Informatics Insights*, *2*(1), 1–10. https://doi.org/10.4137/BII.S2223

Alpiah, S., Asbari, M., Saputri, I. A., & Adilya, N. R. (2024). Oversharing: Urgensi privasi di era digital. *Journal of Information Systems and Management (JISMA), 3*(1), 42-47. https://doi.org/10.4444/jisma.v3i1.877

Anggraeni, S. F. (2018). Polemik pengaturan kepemilikan data pribadi: Urgensi untuk harmonisasi dan reformasi hukum di Indonesia. *Jurnal Hukum & Pembangunan, 48*(4),814–825 https://scholarhub.ui.ac.id/jhp/vol48/iss4/7

Archer, N., Fevrier-Thomas, U., Lokker, C.,

McKibbon, K. A., & Straus, S. E. (2011). Personal health records: A scoping review. *Journal of the American Medical Informatics Association, 18*(4), 515–522. https://doi.org/10.1136/amiajnl-2011-000105

Ardiansyah, M. R., & Ardiana, R. (2023). Kewajiban dan tanggung jawab hukum perdata dalam perlindungan privasi data pasien dalam layanan kesehatan digital. *Hakim: Jurnal Ilmu Hukum dan Sosial, 1*(4), 276-287. https://doi.org/10.51903/hakim.v1i4.1470

Bunga, A. (2015). Kewenangan pemerintah dalam perlindungan hukum pelayanan kesehatan tradisional ditinjau dari Undang-Undang Republik Indonesia Nomor 36 Tahun 2009 tentang kesehatan. *Jurnal Wawasan Hukum, 32*(1), 82–98. https://doi.org/10.25072/jwy.v32i1.91

Coorevits, P., Sundgren, M., Klein, G. O., Bahr, A., Claerhout, B., Daniel, C., Dugas, M., Dupont, D., Schmidt, A., Singleton, P., De Moor, G., & Kalra, D. (2013). Electronic Health Records: New opportunities for Clinical Research. *Journal of Internal Medicine,274*(6),547–560. https://doi.org/10.1111/joim.12119

Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., Putra, R. P., & Saputra, H. (2023). Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal of Social Science Research, 3*(6), 2898-2905. https://doi.org/10.31004/innovative.v3i6.6662

Eckhoff, D., & Wagner, I. (2018). Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys & Tutorials, 20*(1),489–516. https://doi.org/10.1109/COMST.2017.2748998

Effoe, V. S., Katula, J. A., Kirk, J. K., Pedley, C. F., Bollhalter, L. Y., Brown, W. M., Savoca, M. R., Jones, S. T., Baek, J., Bertoni, A. G., & the LIFT Diabetes Research Team. (2016). The Use of Electronic Medical Records For Recruitment in Clinical Trials: Findings from the Lifestyle Intervention for Treatment of Diabetes trial. *Trials*, 17(1), 496. https://doi.org/10.1186/s13063-016-1631-7

El-Gheriani, M., & Hashish, A. (2023). Egypt Amends its Competition Law to Establish A Pre-Merger Control System. *Journal of European Competition Law & Practice, 14*(2),106–112. https://doi.org/10.1093/jeclap/lpad014

Gao, Y., Zhou, Y., Zhou, B., Shi, L., & Zhang, J. (2017). Handling data skew in MapReduce cluster by using partition tuning. *Journal of Healthcare Engineering, 2017*(1). https://doi.org/10.1155/2017/1425102

Greenleaf, G., & Cottier, B. (2021). International

and regional commitments in African data privacy laws: A comparative analysis. *Computer Law & Security Review*, *44*. https://doi.org/10.1016/j.clsr.2021.105638

Hendra, H., Ravel, R., Firdhaus, N., Kurniawan, M. A., & Platina, G. (2021). E-health Personal Data Protection in Indonesia. *Jurnal Hukum Kesehatan Indonesia, 1*(2), 121-131. https://doi.org/10.53337/jhki.v1i02.15

Heriyanto, H. (2023). Analisis perbandingan regulasi dan perlindungan hukum atas privasi data pasien di tiga negara Asia Tenggara (Indonesia, Singapura, dan Laos). *Jurnal Ners, 7*(2), 1247–1259. https://doi.org/10.31004/jn.v7i2.16760

Indriyajati, F., Jawa, M. M. S. D., & Utomo, H. (2023). Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia. *Sanskara Manajemen dan Bisnis,2*(1),59–66. https://doi.org/10.58812/smb.v2i01.130

Iswandari, H. D., & Hoque, S. (2022). Reconceptualizing legal arrangement on the doctor–patient relationship in Indonesia. *Law Reform, 18*(1), 58–78. https://doi.org/10.14710/lr.v18i1.44711

Kesuma, S. I. (2023). Sosialisasi Tentang Ulasan Undang-Undang No. 17 Tahun 2023 Tentang Kesehatan. *Birokrasi: Jurnal Ilmu Hukum dan Tata Negara, 1*(4), 143–156. https://doi.org/10.55606/birokrasi.v1i4.731

Kumar N, M., & Manjula, R. (2014). Role of big data analytics in rural health care – A step towards Svasth Bharath. *International Journal of Computer Science and Information Technologies*, *5*(6), 7172–7178.https://www.ijcsit.com/docs/Volume%205/vol5issue06/ijcsit2014050661.pdf

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology, 38*(1),16–44. https://doi.org/10.1177/02683962221141456

Lestari, A. Y., Misran, M., Raharjo, T., Annas, M., Riskanita, D., & Prabandari, A. P. (2024). Improving healthcare patient data security: An integrated framework model for electronic health records from a legal perspective. *Law Reform, 20*(2), 329–352. https://doi.org/10.14710/lr.v20i2.56986

Lintang, K., & Triana, Y. (2021). Perlindungan Hukum terhadap Hak Privasi dan Rekam Medis Pasien pada Masa Pandemi Covid-19. *Jurnal Hukum Lex Generalis, 2*(10), 913–927. https://doi.org/10.56370/jhlg.v2i10.71

McGraw, D., & Mandl, K. D. (2021). Privacy Protections to Encourage Use of Health-Relevant Digital Data In A Learning Health System. *NPJ Digital Medicine*, *4*(2), 1–11. https://doi.org/10.1038/s41746-020-00362-8

Meinert, E., Alturkistani, A., Brindley, D., Knight,

P., Wells, G., & de Pennington, N. (2018). Weighing Benefits and Risks in Aspects of Security, Privacy and Adoption of Technology in a Value-Based Healthcare System. *BMC Medical Informatics and Decision Making, 18*(100). https://doi.org/10.1186/s12911-018-0700-0

Muntari, M., Djawoto, D., Suwitho, S., & Oetomo, H. W. (2020). Pengaruh Kualitas SIMRS dan Lingkungan Kerja Non Fisik Terhadap Kinerja Pegawai dan Person–Organization Fit (Studi Kasus pada Rumah Sakit Islam Jemursari Surabaya). *JIM: Jurnal Ilmu Manajemen,8*(3),658–674. https://doi.org/10.26740/jim.v8n3.p658-674

Nair, S. C., & Ibrahim, H. (2015). Assessing Subject Privacy and Data Confidentiality in An Emerging Region for Clinical Trials: United Arab Emirates. *Accountability in Research,22*(4),205–221. https://doi.org/10.1080/08989621.2014.942452

Ohoiwutun, Y. A. T., Taniady, V., Lutfian, L., Rachim, K. V., & Putri, N. A. (2024). Euthanasia in Indonesia: Laws, human rights, and medical perspectives. *Law Reform,20*(2),408–430. https://doi.org/10.14710/lr.v20i2.63813

Rahayu, N. (2017). Pengaruh Pengetahuan Perpajakan, Ketegasan Sanksi Pajak, dan Tax Amnesty Terhadap Kepatuhan Wajib Pajak. *Akuntansi Dewantara, 1*(1), 15–30. https://jurnal.ustjogja.ac.id/index.php/akuntansidewantara/article/view/21

Rahmouni, H. B., Essefi, I., & Ladeb, M. F. (2019). Enhanced privacy governance in health information systems through business process modelling and HL7. *Procedia Computer Science, 164*, 706–713.https://doi.org/10.1016/j.procs.2019.12.239

Sarabdeen, J., & Ishak, M. M. M. (2025). A comparative analysis: Health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR). *International Journal of Law and Management*, *67*(1), 99–119. https://doi.org/10.1108/IJLMA-01-2024-0025

Sarabdeen, J., & Moonesar, I. A. (2018). Privacy Protection Laws and Public Perception of Data Privacy: The Case of Dubai E-Health Care Services. *Benchmarking, 25*(6), 1883–1902. https://doi.org/10.1108/BIJ-06-2017-0133

Sarastri, E. S., Saputro, L. T., & Hartini, M. I. (2021). Comparison of aesthetic plastic surgery laws applied in the United States and Indonesia. *Law Reform, 17*(2), 232–251. https://doi.org/10.14710/lr.v17i2.41750

Simamora, I. M. M. (2022). Perlindungan Hukum Atas Hak Privasi Dan Kerahasiaan Identitas Penyakit Bagi Pasien Covid-19. *Sibatik Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan,1*(7).

https://doi.org/10.54443/sibatik.v1i7.126

Situmorang, R. (2022). Hubungan Penerapan Sistem Informasi Pendokumentasian Asuhan Keperawatan Dengan Kepuasan Perawat Di Rumah Sakit Wilayah Jakarta. *Moluccas Health Journal*, *4*(3). https://doi.org/10.54639/mhj.v4i3.967

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum,6*(1),132-142. https://doi.org/10.38043/jah.v6i1.4484

Susanto, S. N. H. (2019). Karakter Yuridis Sanksi Hukum Administrasi: Suatu Pendekatan Komparasi. *Administrative Law and Governance Journal, 2*(1), 126–142. https://doi.org/10.14710/alj.v2i1.126-142

Suyudi, G. A. Wildana, D. T., Prihatmini, S., & Puspaningrum, G. (2025). Kebijakan Formulasi dan Prospektif Penegakan Hukum Tindakan Kealpaan Tenaga Medis/Tenaga Kesehatan (Dinamika Pertanggungjawaban Pidana dalam Malpraktik Medis). *Jurnal Pembangunan Hukum Indonesia*, *7*(2), 49–70. https://doi.org/10.14710/jphi.v7i2.49-70

Taufiqurrohman, A. A., Muhtar, M. H., Ahmad, A., Kasim, N. M., & Imran, S. Y. (2024). The Role of Islamic Law, Constitution, and Culture in Democracy in the UAE and Indonesia. *Ahkam: Jurnal Ilmu Syariah, 24*(1). https://core.ac.uk/download/629902082.pdf

Utomo, H. P., Gultom, E., & Afriana, A. (2020). Urgensi Perlindungan Hukum Data Pribadi Pasien dalam Pelayanan Kesehatan Berbasis Teknologi di Indonesia. *Jurnal Ilmiah Galuh Justisi, 8*(2), 168-185. https://doi.org/10.25157/justisi.v8i2.3479

van Velthoven, M. H., Mastellos, N., Majeed, A., O'Donoghue, J., & Car, J. (2016). Feasibility of Extracting Data from Electronic Medical Records for Research: An international Comparative Study. *BMC Medical Informatics and Decision Making, 16*(90). https://doi.org/10.1186/s12911-016-0332-1

Wang, H., Xu, Z., Fujita, H., & Liu, S. (2016). Towards Felicitous Decision Making: An Overview on Challenges and Trends of Big Data. *Information Sciences*, *367–368*, 747–765. https://doi.org/10.1016/j.ins.2016.07.007

Weber, P. A., Zhang, N., & Wu, H. (2020). A Comparative Analysis of Personal Data Protection Regulations between the EU and China. *Electronic Commerce Research, 20*(3), 565–587. https://doi.org/10.1007/s10660-020-09422-3

Wilona, M. Z., Latifah, E., & Purwadi, H. (2021). Privacy policy on smart contracts in e-commerce transactions. *Law Reform*, *17*(1),47–60. https://doi.org/10.14710/lr.v17i1.37552

Wu, P.-J., & Lin, K.-C. (2018). Unstructured Big Data Analytics for Retrieving E-Commerce

Logistics Knowledge. *Telematics and Informatics,35*(1),237–244. https://doi.org/10.1016/j.tele.2017.11.004

Zhang, Q., & Hansen, D. (2007). Approximate Processing for Medical Record Linking and Multidatabase Analysis. *International Journal of Healthcare Information Systems and Informatics, 2*(4), 14. DOI: 10.4018/ jhisi.2007100104

BOOKS

Amiruddin, A., Asikin, Z. (2012). *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo Persada.

Institute of Medicine (US) Roundtable on Value & Science-Driven Health Care. (2010). *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary*. Washington, DC: National Academies Press (US). http://www.ncbi.nlm.nih.gov/books/NBK54302/

Mittelstadt, B. D., & Floridi, L. (Eds.). (2016). *The ethics of biomedical big data*. Cham, Switzerland: Springer International Publishing. https://doi.org/10.1007/978-3-319-33525-4

Yustina, E. W. (2012). Mengenal Hukum Rumah Sakit. Bandung: C.V. Keni Media.

LAWS & REGULATIONS

DPD PORMIKI DKI Jakarta. (2025). Regulation of the Minister of Health of the Republic of Indonesia Number 269/Menkes/Per/III/2008 about Medical Records. Retrieved from https://pormikidki.or.id/lain-lain/download/26-permenkes-269-tahun-2008-rekam-medis

Database Peraturan JDIH BPK. (2025a). Law Number 29 of 2004 concerning Medical Practice Republic of Indonesia. Retrieved from https://peraturan.bpk.go.id/Details/40752/uu-no-29-tahun-2004

Database Peraturan JDIH BPK. (2025b). Law Number 27 of 2022 concerning Personal Data Protection Republic of Indonesia. (2022). Retrieved from https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

United Arab Emirates. (2019). Federal Law No. 2 of 2019 on the Use of Information and Communication Technology (ICT) in Health Fields. Retrieved from https://uaelegislation.gov.ae/en/legislations/1209/download

United Arab Emirates. (2021). Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. Retrieved from https://uaelegislation.gov.ae/en/legislations/1972/download

TECHNICAL REPORT

Laney, D. (2001). 3D Data Management: Controlling Data Volume, Velocity and Variety. *META Group Research Note,*

6(70), 1. https://diegonogare.net/wp-content/uploads/2020/08/3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

UNDERGRADUATED THESIS

Rifly, N. F. (2022). Analisis Pengaruh Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) Terhadap Kinerja Karyawan di Unit Rawat Jalan RSUD Arifin Achmad Provinsi Riau. Undergraduate Thesis: Universitas Awal Bros. https://repository.univawalbros.ac.id/96/

CONFERENCE

Ghandour, A., & Woodford, B. J. (2019). Ethical Issues in Artificial Intelligence in UAE. In 2019 International Arab Conference on Information Technology (ACIT) (pp. 262–266).https://doi.org/10.1109/ACIT47987.2019.8990997

PROCEEDING

Paxton, C., Niculescu-Mizil, A., & Saria, S. (2013). Developing Predictive Models Using Electronic Medical Records: Challenges and Pitfalls. *AMIA Annual Symposium Proceedings,*pp.1109–1115. https://europepmc.org/articles/PMC3900132

ONLINE SOURCES

DA, A. T. (2021). Diduga Data Peserta Bocor, Begini Upaya Yang Dilakukan BPJS Kesehatan. Retrieved from https://www.hukumonline.com/berita/a/diduga-data-peserta-bocor--begini-upaya-yang-dilakukan-bpjs-kesehatan-lt60aca63a21b82/

GDPR.EU. (2018). What is GDPR, the EU's new data protection law? GDPR.eu. Retrieved from https://gdpr.eu/what-is-gdpr/

Ivan, D. (2019). Clinical vs. consumer data: Why does it matter?. Retrieved from https://www.chiefhealthcareexecutive.com/view/clinical-vs-consumer-data-why-does-it-matter

Sanjoyo, R. (2007). Aspek Hukum Rekam Medis. D3 Rekam Medis FMIPA Universitas Gadjah Mada. Retrieved from https://www.academia.edu/19696792/ASPEK_HUKUM_REKAM_MEDIS

Tithecott, A., & Jhala, K. (2019). The Federal Law Regulating The Use of Information and Communication Technology in the UAE Healthcare Sector. Retrieved from https://www.tamimi.com/law-update-articles/the-federal-law-regulating-the-use-of-information-and-communication-technology-in-the-uae-healthcare-sector/

UAE - Data Protection Overview. (2022). Retrieved from https://www.dataguidance.com/notes/uae-data-protection-overview