Advanced Digital Services in Health: Global Insights on Security and Privacy Issues

Dimitrios D. Vergados and Eleni Varvarousi(✉)

Department of Informatics, University of Piraeus, 80, Karaoli & Dimitriou St., Piraeus, Greece
{vergados,varvaroussi}@unipi.gr

Abstract. The objective of this research is to provide an overview of digital services in the health sector. The emergence of innovative digital services has been accompanied by a multitude of issues and problems pertaining to privacy and security. To effectively tackle the issues around privacy and security in the realm of digital health, it is important to consider the principles established by international organizations. Moreover, a thorough analysis of the existing regulatory framework and unresolved issues in digital health is essential. Addressing these challenges effectively requires a unified approach that can lead to the implementation of robust solutions. Furthermore, this paper discusses the obstacles both developed and developing countries face regarding digital health, underscoring the need for a unified and international viewpoint.

Keywords: digital health · artificial intelligence · DHIS 2 · security · privacy · mobile health applications

1 Introduction

Digital health plays a crucial role in supporting the attainment of the United Nations' Sustainable Development Goals (SDGs), especially as regards SDG 3, which aims to provide universal access to healthcare and the improvement of people's health, regardless of age.

In recent years, nations have developed their own digital health policies and initiatives. The digital transformation of the health care sector is comprised of numerous technologies designed to facilitate a unified patient experience. The purpose of digital health technologies is to improve the state of one's well-being. Robotic surgery, wearable health devices, mobile health apps, remote monitoring of patients, artificial intelligence (AI) and machine learning, internet of medical things (IoMT), the use of nanotechnology for use in diagnosis or therapy, virtual reality (VR) and augmented reality (AR), blockchain systems, telemedicine, virtual health assistants and 3D printing are only a few of the many advancements in technology that have been developed in the healthcare sector. However, the utilization of disruptive technologies come with a set of challenges that are important to address and comprehend for the successful integration and maximization of the benefits of these technologies.

L. A. Maglaras and C. Douligeris (Eds.): WiCON 2023, LNICST 527, pp. 47–62, 2024.
https://doi.org/10.1007/978-3-031-58053-6_4

The World Health Organization (WHO) presented a Global Strategy focusing on digital health, underscoring the pivotal role of technological tools in meeting health-related objectives set by the Sustainable Development Goals. The Global Digital Health Strategy for 2020–2025 by the WHO underscores that for digital health solutions to be truly effective, they must not only be user-friendly but also foster universal and fair access to health services. Moreover, these tools should bolster health systems' capability to deliver cost-friendly, equal treatment while prioritizing the privacy and confidentiality of patient's data and the security of health-related information [1].

Additionally, the WHO emphasizes the importance of data security and highlights the need for transparency, scalability, and replicability, all while grounding these principles in equality and sustained relevance [1]. It should be highlighted that cooperation between developers, regulators, international organizations and entities is crucial to the development of innovative digital solutions for health, with a particular emphasis on privacy, data protection, data quality and transparency and the development of robust and consistent standards, among other factors. In a period where the health sector is increasingly digital and transcends geographical boundaries, fostering global synergies becomes crucial.

Digital health solutions should evolve by considering a comprehensive range of issues, including socio-economic aspects, technological advancements, cultural nuances, ethical standards, environmental considerations, legal frameworks and policy directives. These diverse considerations are instrumental in shaping truly effective and inclusive health solutions. As such, underscoring the significance of comprehensive global health solutions is pivotal, ensuring that health technologies benefit every individual in a holistic and equitable manner.

2 Digital Health

The digital health ecosystem is dynamic and complex. In general, it is possible to classify the evolution of healthcare into five distinct periods. Health 1.0 was primarily centered on the role of the doctor, Health 2.0 included electronic medical record histories, Health 3.0 shifted towards the patient emphasizing their active involvement in healthcare [2]. In the Health 4.0 framework, there's a blend of modern tools, mainly focused on the application of AI techniques [3]. Subsequently, the advent of healthcare 5.0, introduced digital health services such as wellness monitoring, emotional telemedicine, as well as smart self-management and various other innovative approaches to healthcare delivery [4].

There are several definitions concerning digital health. Particularly digital health can be defined as the integration of information technology into healthcare. This encompasses systems used in medical facilities like hospitals and clinics, as well as applications owned and used by patients [5]. After thorough research, it's evident that most of these definitions highlight the utilization of technological advancements to improve individual and community health. Furthermore, they also emphasize the enhancement of patient engagement by intelligently analyzing clinical and genetic data [6]. Several fundamental characteristics are vital to the functioning of digital health. Privacy and security, the accessibility of digital health technologies and tools, are merely a few of these. In recent

years, numerous global initiatives and policies related to digital health have arisen. The World Health Organization (WHO) and the International Telecommunications Union (ITU) in the realm of global health and digital technology promote technologies and strategies, advocate policies and international standards that facilitate coordination as well as research and development. Furthermore, interactive digital tools like the Global Digital Health Index helps in benchmarking and comparing digital health advancements. Additionally, collective initiatives like the Health Data Collaborative underscore the global commitment to advancing digital health. But when examining global indicators on legislation, policy, compliance, infrastructure, leadership, governance, services, applications, strategy, investment and interoperability standards for digital health, it is evident that that there is no universal approach to digital healthcare and management, leading to notable disparities among nations. Digital health is a dynamic domain, leveraging technological advancements to revolutionize healthcare while also addressing prominent global challenges.

2.1 Artificial Intelligence in Healthcare

The integration of artificial intelligence (AI) into the domain of digital health represents a noteworthy transformation in healthcare and brings substantial changes in multiple aspects of society. This development carries far-reaching implications for diverse domains including diagnostics and imaging, predictive analytics, treatment, operation, drug development, remote monitoring and wearables, natural language processing (NLP), telemedicine, telehealth and remote diagnostics. The use of artificial intelligence and related technologies within the healthcare sector has been further expedited by the COVID-19 pandemic [7]. Owing to the prevalent use of artificial intelligence in the healthcare sector, the European Commission has introduced various initiatives. One such initiative is the establishment of the European Commission's High-Level Expert Group on Artificial Intelligence. This group has laid down guidelines to ensure trustworthy Artificial Intelligence [8]. An AI system to be secure, needs to follow among others legal, ethical principles and system robustness. Furthermore, human oversight, technological reliability, safety, data protection, accessibility, encouragement of diversity, promotion of fair treatment, accountability and responsibility are all necessary elements [9]. AI platforms ought to be reliable and secure but also safeguard people's constitutional rights. Data security and user privacy should be guaranteed by means of data management processes and ensure transparency, accessibility, openness, sustainability and accountability.

There are different methods which are frequently used in artificial intelligence means of digital health as machine learning methods, neural networks, deep learning methods. Deep learning as defined by ITU [ISO/IEC 22989] is an approach aiming at creating rich hierarchical representations through the training of neural networks with many hidden layers [10]. Deep learning has introduced sophisticated methods and tools for addressing complex health-related issues. For instance, deep learning is often used to find harmful tumors in imaging pictures or in radiomic, to process natural language (NLP) as well as in robotic process automation (RPA) [11].

Deep federated learning-based machine techniques are employed in the healthcare sector and are currently in developmentwith the use of models that maintain data at a

local level and prevent exchange of information [12, 13]. This decentralized approach is particularly beneficial for privacy and data security assurance and is often selected for the retention of data. It aims at precise localization services that claim to prioritize the protection of users' privacy and security. These services use training methods that rely on resilient and privacy-preserving decentralized deep federated learning (RPDFL) strategies [14]. One notable example is its use in identifying Alzheimer's disease of individuals [15]. By leveraging this decentralized approach, medical professionals can analyze data from diverse sources without compromising patient privacy, leading to more accurate and timely diagnosis.

Furthermore, in recent years, the integration of AI in the medical sector has been notably evident in smartwatches that encompass a broad spectrum of functionalities. For example, they provide health tracking, fitness advice, seamless communication options, efficiency tools, data-driven forecasts, user-friendly interfaces, mental well-being assessments, directional aids and instant health notifications. Smartwatches have emerged as essential tools in the realm of health management, offering a range of monitoring capabilities to those facing different medical issues. For instance, according to various studies they can assist in the detection pertaining to skin cancer. These devices with the integration of advanced sensors and computational techniques, provide early detection and regular dissemination of alerts, positioning them as vital associates in preventive healthcare methods [16]. The use of AI in healthcare is significant and the issues that have been addressed up to this point just serve as examples of the challenges that relate to its utilization. In the following section some further instances of the use of artificial intelligence will be analyzed as regards the healthcare domain and the role of AI in identifying diseases.

It is important to note, however, that the use of AI in the diagnosis of illness is more prevalent in industrialized nations owing to the progress that has been made in healthcare infrastructure and resources. Furthermore, it is essential to emphasize, however, that the widespread use of information systems in developing countries helps to improve healthcare accessibility as well as disease monitoring to bridge the gap with the advantages of digital health applications.

2.2 Applications of Digital Health in Dynamic Economies

The introduction of artificial intelligence (AI) into the medical field is undergoing a transformation that is having a dramatic impact on the practice of healthcare across all its separate sectors. Therapeutic techniques, diagnostics, patient care management medical imaging technology are only some of the applications that may be used which demonstrate the technology's obvious potential for boosting patient treatment and refining medical procedures.

A notable example is the use of artificial intelligence (AI) in gastroenterology, which has expanded significantly in recent years. Applications of artificial intelligence are used for detection, diagnosis and treatment of gastrointestinal (GI) diseases that include endoscopic procedures, image analysis in radiology, predictive analytics, pathology, personalized treatment and monitoring.

The applications of AI technologies in gastroenterology are broad. For instance, the use of computer-aided detection (CADe) in the identification of polyps has promised

in serving as an additional observer, hence mitigating the likelihood of polyp detection errors [17]. Furthermore, various artificial intelligence (AI) technologies are developed for the purpose of facilitating endoscopic procedures, namely colonoscopies.

Endoscopic and colonoscopic robotic surgery offers hope for many promising results, as is the case in other domains such as in digital orthopedic surgery. With the most recent advancements in robotics, the creation of new therapies for diseases and diagnoses, may improve patient accessibility to care and treatment outcomes. Furthermore, with the use of AI there is assistance in navigation, in tracking and cording of the procedure, in quicker intervention during the surgery practice. Whereas the conventional approach to clinical endoscopy relies on the doctor's expertise and training in performing biopsies, the use of artificial intelligence during gastroscopies, leads to enhanced diagnostic precision. Innovative approaches that make use of artificial intelligence during gastroscopies performed in recent years, result in increased diagnostic accuracy as well as detection of many illnesses, including stomach cancer. It's widely acknowledged that stomach cancer can rapidly advance towards a malignant state. The earliest symptoms of the phenomenon often exhibit subtlety and may evade discovery, hence emphasizing the criticality of early identification and action for enhanced results. With the use of a gastroscope based for instance on GCN (Graph Convolutional Networks), this novel detection model for early malignant lesions, according to studies, has effective results when compared to conventional medical methods [18, 19].

Moreover, AI is employed in medical and mobile health applications for various purposes, including remote patient monitoring, disease diagnosis and mental health support. At present, the market offers a wide array of healthcare applications, with a staggering number exceeding 350,000 at a global scale [20]. Furthermore, their diverse range of capabilities to aid patients in self-management contributes to their awareness as having significant potential in the treatment of acute pain and chronic diseases. The medical health applications are utilized extensively in gastroenterology to treat patients with diabetes or chronic liver disease (CLD) [21]. Furthermore, medical health apps also provide educational material for patients. In the discipline of gastroenterology, these apps are used to optimize gastrointestinal preparation prior to colonoscopy. Consequently, this ultimately results in an enhancement in the overall efficacy of this procedure and guarantees a comprehensive purification of the colon prior to the intervention. Research has shown that optimizing intestinal cleansing significantly improves the detection rate of polyps and reduces the likelihood of complications. This is of great significance due to statistical evidence indicating that 25% of individuals undergoing colonoscopy exhibit poor gastrointestinal cleaning, prior to the intervention, resulting in reduced accuracy of the obtained results [22]. The observed improvement in therapeutic outcomes may be attributed to the increase in patients' knowledge. Furthermore, it is worth noting that the mobile health apps offer significant advancement in the management of chronic illnesses. In addition, digital biomarkers assume a pivotal role in the management of cancer patients by offering enhanced prognostic information in comparison to conventional techniques.

Additionally, the prevalence of telemedicine and telehealth in gastroenterology is significant due to the chronic nature of many digestive disorders, such as liver cirrhosis. This is also the case with telemedical instruments for inflammatory bowel disease, chronic liver disease, patients undergoing liver transplantation or diabetic patients.

But as highlighted earlier, it's essential to note that the uptake and implications of artificial intelligence differ markedly between nations throughout the globe. Infrastructure, economic conditions and data accessibility are among the factors that contribute to the disparities.

According to the findings of the Organization for Economic Co-operation and Development (OECD), a total of sixty-nine (69) nations have established regulatory and legislative frameworks related to the use of artificial intelligence (AI). It is worth noting that most of these nations are high-income nations [23]. Furthermore, it should be stressed that when investigating the topic of digital health, it is essential to acknowledge the widespread adoption in developing countries as well. This is vital because of the numerous potential benefits that the digital health applications offer, not only for the global community but also for ensuring inclusion in digital health. Inclusion is a necessity, particularly considering the challenges faced in achieving the UN Sustainable Development Goals (SDGs) adopted by all UN member states in this domain.

2.3 Applications of Digital Health in Developing Nations: The District Health Information System 2

An important application of digital health in "developing nations" is seen in the implementation of health information systems, that have an important part in global digitization efforts. These systems are mostly required for effective health information management.

The District Health Information System 2 (DHIS 2) is the largest health information management system that has been designed as an innovative solution for enhancing the effectiveness of health management information systems (HMIS). The implementation of this Health Information System in several developing countries worldwide has been supported by International Organizations and the Norwegian government, underscoring the notable advancements achieved. DHIS 2 is used by 114 nations for the purpose of gathering and evaluating health data, including a population of 3.2 billion persons, which accounts for about 40% of the world's population. Furthermore, DHIS 2 is provided at no cost as a global public benefit [24]. It has been used for a wide range of health-related reasons by national health ministries, international development organizations and non-governmental organizations throughout the globe. DHIS 2 is employed in various fields, which include health management information systems (HMIS), disease surveillance and early warning, patient health records and tracking, supply chain management, program monitoring and evaluation, health workforce management, mobile health (mHealth) initiatives, health finance and budgeting, geospatial analysis and mapping, as well as integration with other systems.

The DHIS 2 platform is founded upon the principles of open data, which gives rise to several difficulties pertaining to privacy rights, confidentiality and data preservation. The susceptibility of DHIS 2 to corruption and deceit arises from several factors, including constraints in digital infrastructure, regulatory frameworks, and operational capabilities. However, it is important to note that DHIS 2 also has the capacity to contribute towards the prevention and mitigation of corruption and deception [25]. This assertion has validity because of the lack of comprehensive laws regarding data protection and privacy, particularly in nations with lower and moderate economic levels. For instance, in year 2016, a data breach took place in Sao Paulo, resulting to unauthorized disclosure

of personal information and medical records related to 650,000 individuals who went through pregnancy and abortion treatment. Because of the current legislative structure in Brazil, in which abortion is illegal, women and medical practitioners affected by data breach were exposed to criminal prosecution threat [25].

The DHIS 2 platform incorporates machine learning techniques, hence presenting many difficulties pertaining to privacy and security. Moreover, with respect to the system, there is a recurring discourse around the application of data and the need to scrutinize the individuals or organizations who utilize this data [26]. The effective deployment of DHIS 2 requires an enormous and significant undertaking, demanding substantial political commitment across different levels of management. This initiative serves as a crucial element for disease surveillance and reporting systems, aiming to improve compliance, ensure longevity and safeguard the civil liberties of individuals [27].

Throughout the years, the District Health Information System (DHIS) has gradually supplied vital information for health care planning, monitoring, and reporting. The advancement of the Health Management Information System (HMIS) is focused on this component, which is significant. For instance, in South Africa the debut of DHIS in 1996/1997 as an ongoing system for monitoring health care delivery in the public health sector was an important turning point. South Africa successfully moved from DHIS 1.4 to WebDHIS, both of which are essential components of the health sector's overall Health Management Information System (HMIS). South Africa upgraded smoothly from DHIS 1.4 to WebDHIS [28]. But like any digital platform, DHIS 2 faces challenges related to security and privacy and in particular data breaches, data integrity, data transmission and software vulnerabilities.

3 Open Issues in Digital Healthcare

3.1 Privacy and Security Challenges

Security and privacy risks present serious challenges across the field of digital health. Data breaches and the unauthorized disclosure of personal data are common incidents within the digital health industry and security breaches are the primary source of threats to cybersecurity. The European Union Agency for Cybersecurity (ENISA) has conducted the examination of incidents in compliance with the Network and Information Security Directive [29]. The Cybersecurity Incident Reporting and Analysis System (CIRAS) [30], designed to facilitate incident reporting between member states presents interesting findings as regards the status among EU member states. Based on the most recent data published by the European Union Agency for Cybersecurity (ENISA), it is revealed that around 32% of incidents resulting in substantial consequences were seen within the Healthcare Sector [31]. Specifically, most instances, making up 53%, have been determined to involve medical personnel. It is noteworthy that European hospitals witnessed a significant percentage of incidents, involving 42% of the total amount of incidents. Health authorities, organizations, and agencies have been identified to be involved in 14% of the incidents, while medical companies were identified as being involved in 9% of the incidents. Most documented occurrences resulted in either data breaches or loss, accounting for 43% of the cases. Additionally, there were instances of healthcare service interruptions, which constituted 22% of the incidents. Furthermore, the European

Union Agency for Cybersecurity (ENISA), in its recent study, underscored the increasing severity of vulnerabilities found in digital wearable devices that store personal data [31].

The reliability of these devices may have a substantial influence on the health outcomes of patients, perhaps resulting in inaccurate diagnosis or inappropriate therapies. Smart health applications, utilizing smart devices pose greater security and privacy risks than conventional computing systems due to their heterogeneity, scalability, and dynamic assets. In general, these devices can collect data, store data and transmit to different systems by means of Wi-Fi connection [32]. The utilization of artificial intelligence (AI) algorithms is crucial for the comprehension and analysis of enormous amounts of information in a wide range of fields. Algorithms function at a significantly faster rate in contrast to human beings, permitting them to identify patterns, trends and irregularities which may evade manual evaluation [16]. However, the utilization of data presents substantial challenges, and it is frequently observed that there is no obvious difference among data pertaining to medical treatment and not medical treatment data [32]. Additionally, while collecting users' medical information via wireless connections and complex algorithms, developers frequently neglect to account for sensitive data security issues [33, 34]. Moreover, there's a common misconception stemming from their regular linkage with other applications or GPS tools. As a result, these methods often result in erroneous conclusions and engender the assurance of confidentiality and data privacy. Little regulation governs the digital health footprint and data analysts derive health assumptions from frequently collected data [35]. As a consequence, false assumptions are in common because they are frequently linked to other applications or GPS trackers.

Within the domain of healthcare, it is imperative to reinforce devices and systems against a variety of threats that fall into distinct categories, including but not limited to responsibility tracking, indisputable transactions, system reliability, resilience to setbacks, robustness and fault tolerance. Three fundamental principles form the basis of security requirements: confidentiality assurance, integrity maintenance and system availability guarantee. In general, potential privacy risks can be categorized as follows: apprehensions regarding location-based privacy, the prospect of impersonation, data interception, the way data is stored, inadequate testing, timely updates of devices, the absence of continuous device surveillance and the participation of anonymous users within the technological ecosystem.

Safeguarding medical data is complicated. In the past, various mechanisms such as encryption, blockchain, and biometrics have been utilized to address privacy concerns. Even though blockchain mechanisms have a significant impact on the healthcare industry and could help protect data privacy and security while ensuring information accuracy [16], contrary to this, numerous studies have shown that blockchain-based medical systems frequently lack privacy and security [36]. Transmission as well as storage, along with established security criteria should aim at maintaining data confidentiality, integrity, accessibility, and availability along with authenticity and non-repudiation and the use of security protocols.

In addition to encryption methods, the domains of machine learning (ML) and deep learning (DL) are critical components in the development of intelligent applications that place a premium on authentication of users and confidentiality. It is widely recognized

that they effectively prevent unauthorized access to applications that take advantage of the features of intelligent devices and big data. Security-focused and privacy-enhancing technologies must be integrated during the design phase. Once these cutting-edge technologies have been integrated, they can be implemented in a variety of systems. To ensure that a system is resistant to threats, it is critical to implement severe security engineering practices from the outset. This fundamental stage guarantees that the following levels of the system are strengthened and resistant to potential vulnerabilities [37].

Furthermore, it is critical to incorporate ethical, governance, and regulatory considerations in an integrated way throughout the entire developmental process of artificial intelligence, encompassing its inception, conception, design, development, and ultimate integration. Ensuring the confidentiality and integrity of data within the realm of digital health is not merely an essential technological requirement; it is fundamental to maintaining the trustworthiness of healthcare infrastructures. By implementing these security precautions, resilience of healthcare systems as well as support of the confidence that patients have in them is assured. Likewise, this trust serves as the foundation for providing effective patient care and enables advancements in the field of digital health innovation.

3.2 Regulatory Framework Challenges

In accordance with international human rights obligations, the WHO resolution on digital health urges member states to "develop, as appropriate, legislation and/or data protection policies concerning issues such as data access, sharing, consent, security, privacy, interoperability, and inclusivity" [38].

Moreover, the current EU legal framework intends to increase the effectiveness and quality of protection of privacy and personal data processed in connection with electronic communications, as well as provide greater legal certainty for citizens. The objective of digital health is to become an essential element of health agendas, with the intention of providing ethical, safe, secure, reliable, fair and sustainable advantages to individuals. Furthermore, it aims to be developed with principles of transparency, accessibility, scalability, replicability, interoperability, privacy, security and confidentiality. In the event of an emergency, special rules should be considered. Regarding the privacy and security of digital healthcare as well as global strategic objectives, countries try to implement legal and ethical structures to ensure patient safety, secure health data, ensure appropriate usage and ownership of medical data, protect data privacy, facilitate data recovery, and protect intellectual property rights.

The current regulatory framework includes among others Directive 2011/24/EU, telemedicine acts, digital healthcare provisions, e-health action plans, NIS2, interoperability framework and GDPR. Furthermore, the regulatory proposal, which was unveiled in May 2022 by the European Commission, aimed to create a specialized ecosystem known as the European Health Data Space (EHDS) to accommodate health data. Ratification of the EHDS would create a framework that ensures the complete standardization of electronic patient records across the European Union and streamline the process of transferring such records between Member States. These measures aim to improve collaboration among member states, build trust in data privacy and security, and leverage the potential of cloud services.

Furthermore, ethical standards for the development of trustworthy artificial intelligence have been set up by Expert and Focus Groups such as the High-Level Expert Group on Artificial Intelligence operating under the auspices of the European Commission. Focus groups and initiatives also stress the importance of regulatory challenges aiming at harmonization among the nations. For instance, the ITU AI Focus Group on Artificial Intelligence for Health [39] prioritizes regulatory principles pertinent to AI in the healthcare sector. It emphasizes the importance of employing a comprehensive strategy that incorporates the entire product lifecycle, with risk management, meticulous design, privacy, and data security as top priorities. This statement emphasizes the importance of external validation and stakeholder engagement for the successful deployment of an AI system.

The field of digital health encounters a multitude of regulatory obstacles because of a swift in technological progress, the establishment of limits, safeguarding data privacy and security, ensuring interoperability, validating clinical efficacy, addressing global disparities, establishing reimbursement frameworks, considering ethical implications, conducting post-market monitoring, and fostering collaboration among stakeholders. The rapid rate at which technical innovations occur often surpasses the capacity of regulatory entities to assess and establish rules, resulting in deficiencies in supervision, possible hazards for patients and obstacles to innovation. Ensuring patient safety and promoting innovation within the digital health landscape necessitates the prioritization of certain key elements, such as safeguarding data privacy and security, enabling interoperability, acknowledging ethical considerations, and evaluating other pertinent issues. The European Commission's prioritization of safe, secure, and trustworthy digital health technologies, together with the implementation of the AI Act, requires sufficient time to effectively address the potential hazards and misuse of technology and safeguard civil rights. Furthermore, it is important to note that although the European Union has implemented extensive legislation regarding consumer digital privacy, the United States has not yet enacted a comprehensive legislative framework.

The United States has implemented a sector-specific approach, whereby varying levels of security are granted to health care under the Health Insurance Portability and Accountability Act (HIPAA) [40]. State governments throughout the United States are enacting privacy legislation at an accelerated rate. States such as Connecticut, Utah, California, Virginia, and Colorado are among those that have thus far enacted comprehensive legislation regarding data privacy. Additionally, protective measures are in place to ensure the confidentiality of genetic data, which is particularly delicate, in compliance with the Genetic Information Nondiscrimination Act (GINA). It should be noted that it is often stated that the regulations fail to govern significant aspects of digital consumer privacy [41]. Furthermore, the absence of standardization in eHeath interventions often gives rise to a multitude of challenges within the health sector.

Currently, there is a scarcity of effective international regulations concerning smartphone applications, including those that function as diagnostic or therapeutic tools or as medical applications [21]. It is critical to emphasize that a significant number of health applications lack adequate data security protocols, a prerequisite for safeguarding the data's confidentiality. Additionally, a mechanism that would allow end users to discern which items conform to superior security standards compared to industry standards,

thereby confirming their suitability for secure utilization, has yet to be established. In addition, regarding interoperability issues, it is often observed that data is stored in separate locations that lack the necessary compatibility. Standardized interfaces and interoperability standards that are universally acknowledged are therefore essential to ensure the efficient integration of digital advancements within the medical domain [42].

Looking at digital health from a global perspective, there are numerous regulatory barriers which hinder the progress, operation, and integration of digital health systems in developing countries. In several developing countries, digital health regulations are fragmented, with numerous agencies exercising authority without clearly defined responsibilities. Therefore, a regulatory framework that is fragmented could hinder the implementation of digital health technologies. In India, for instance, there is no clear framework that outlines the functions of the multiple bodies in charge of regulating digital health, resulting in a regulatory overlap. The Central Drugs Standard Control Organization (CDSCO), the Ministry of Health and Family Welfare (MoHFW) and the Ministry of Electronics and Information Technology (MeitY) are all responsible for various issues that cause regulatory confusion, delays, or overlaps [43]. Moreover, inadequate cybersecurity and data privacy policies pose substantial threats to developing-country digital healthcare systems. In 2022, for example, Indian Healthcare experienced 1.9 million cyberattacks [44]. Regulatory barriers for digital health in developing nations include disordered regulation, the absence of insurance coverage regulatory mechanisms, the increased complexity of regulation due to the diversity of digital health tools, inadequate data protection laws and a dearth of regulatory staff expertise [45]. For example a systematic evaluation conducted in Ethiopia identified inadequate infrastructure as a significant impediment to the implementation of electronic health records [46].

Developing countries frequently have disorganized digital health regulations, which results in fragmented guidelines and legal ambiguities. Regulatory bodies are frequently overtaken by technological advancements, which complicates the regulatory process. The regulation of digital health instruments is additionally complicated by their heterogeneous character, encompassing mHealth applications, wearables and EHRs. In addition, it is difficult to determine whether these instruments qualify as medical devices. Inadequate technical expertise further impedes effective implementation and oversight [45].

Digital revolution presents several regulatory issues for developing nations. The management of regulatory assets demands a careful balance between innovation and policy compliance. Lack of technical competence makes compliance with international and local standards difficult. The lack of data protection and privacy legislation and changing cybersecurity and healthcare rules exacerbate matters. The variety of digital instruments being used, each with its own regulations, add to this complexity. Innovation and research are essential for success, but developing nations frequently lack comprehensive rules to govern their implementation and scaling. All the above mentioned issues highlight the need for stronger, clearer and more supportive regulatory structures to help these countries use digital technologies safely and effectively.

Table 1. Digital health challenges in developing vs developed nations

Developing nations		Developed nations	
Technical Assets	Regulatory assets	Technical Assets	Regulatory assets
Interoperability	Policy frameworks	Workforce training and change management	Technology adoption
Data Management	Compliance standards	Interoperability	Unregulated software apps
Limited Infrastructure	Insufficient technical knowledge	Advanced telehealth infrastructure	Ethical issues in AI and Big Data
Financial Constraints and digital divide	Inadequate data protection and privacy laws and cybersecurity healthcare regulations	Wearable health technologies	AI and machine learning regulatory framework
Data privacy and security	Regulatory divergence	Data privacy and security	Cross border data sharing
Connectivity	Innovation and research policies	Data quality and standardization	Cybersecurity requirements

4 Conclusion

Technological advances have the potential to bring about significant improvements, however, they are accompanied by several obstacles, such as data privacy concerns, difficulties in integrating new technologies into existing healthcare systems and complexities in regulatory frameworks. It is not enough to rely solely on technological solutions to protect an individual's right to privacy. Human factors, as well as policies and incentives, must be given the highest priority to achieve the desired results. To facilitate the seamless integration of technology into the healthcare sector, it is crucial to strengthen legal, ethical, and regulatory frameworks.

It is of the utmost importance that the requirements for information technology and governance are arranged to be compatible. With a unified strategy, data interoperability in healthcare systems may be addressed. It is crucial that nations should re-examine their current legal and ethical frameworks for preserving the security of health data, the appropriate use and ownership of medical data and the privacy and confidentiality of data.

Given the intricacies of the digital health domain, it is essential to approach the subject from a worldwide standpoint, recognizing the need for international collaboration to enable the secure advancement and utilization of digital health applications. Various stakeholders could maintain ongoing collaboration to foster common understanding, in conjunction with established national and international entities, to address digital health and artificial intelligence (AI)-related subjects. This collaboration is crucial for achieving convergence and harmonization of necessary legislative prerequisites as well

as adopting the standards necessary to avoid privacy leakage and loss of confidentiality assurance.

Upon review of the domain of digital health, it becomes apparent both developing and developed countries face significant disparities and distinct challenges. Developing countries face a range of obstacles, such as limited technical resources and infrastructure, barriers to achieving interoperability, and complexities associated with data management. Beyond financial constraints and the digital divide, further impediments include concerns related to data security, cybersecurity and the maintenance and enhancement of connectivity. Challenges posed by regulations, inadequate data protection legislation, regulatory divergence including limited technical expertise as well as the complexity introduced by advanced digital services, present major challenges further development.

On the other hand, developed nations face a unique set of challenges, regardless of their advanced technological capabilities and regulatory frameworks. These encompass the imperative for change management to adapt to the rate of technological advancement and ethical issues pertaining to advancements in digital health. The current regulatory framework, the management of cross-border data sharing, data security and confidentiality of data are all crucial concerns. Furthermore, developed nations are faced with the simultaneous predicaments of addressing data quality and standardization concerns, ensuring interoperability among health systems and managing the unregulated nature of software applications. Both industrialized and developing countries face intricate challenges in the field of digital health. To foster a more inclusive and efficient global health ecosystem, it is vital that they mutually gain from each other's insights.

Acknowledgement. This work has been partly supported by the University of Piraeus Research Center (UPRC).

References

1. World Health Organization. Global Strategy on Digital Health 2020–2025, vol. 2021, p. 10. WHO, Geneva (2021). ISBN 978-92-4-002092-4
2. Jayaraman, P.P., Forkan, A.R.M., Morshed, A., Haghighi, P.D., Kang, Y.-B.: Healthcare 4.0: a review of frontiers in digital health. WIREs Data Min. Knowl. Discov. **10**, e1350 (2020). https://doi.org/10.1002/widm.135
3. Hathaliya, J.J., Tanwar, S.: An exhaustive survey on security and privacy issues in Healthcare 4.0. Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, 382481, India
4. Mbunge, E., Muchemwa, B., Jiyane, S., Batani, J.: Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. Glob. Health J. **5**(4), 169–177 (2021)
5. Fatehi, F., Samadbeik, M., Kazemi, A.: What is Digital Health? Review of Definitions, vol. 275: Integrated Citizen Centered Digital Health and Social Care, Studies in Health Technology and Informatics, The European Federation for Medical Informatics (EFMI) and IOS Press (2020)
6. Paton, C.: BMBS BMedSci MBA FFCI, Textbook of Digital Health, University of Oxford, Oxford, UK
7. Wittbold, K.A., et al.: How hospitals are using AI to battle Covid-19. Harvard Business Review (2020). https://hbr.org/2020/04/how-hospitals-are-using-ai-to-battle-covid-19

8. European Commission's High-Level Expert Group on Artificial Intelligence. Ethics guidelines for trustworthy AI (2020). https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
9. Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence, European Commission, Brussels (2019)
10. Definition by ITU-T Focus Group Focus Group on Artificial Intelligence for Health, FG-AI4H DEL0.1 Common unified terms in artificial intelligence, 09/2022, International Telecommunication Union, Standardization Sector, FG-AI4H DEL0.1 for health (FG-AI4H) (2022)
11. Davenport, T., Kalakota, R.: The potential for artificial intelligence in healthcare. Future Health J. **6**(2), 94–98 (2019). https://doi.org/10.7861/futurehosp.6-2-94. PMID: 31363513; PMCID: PMC6616181
12. Mandal, K., Gong, G.: PrivFL: practical privacy-preserving federated regressions on high-dimensional data over mobile networks. In: Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, pp. 57–68 (2019)
13. Wu, W., He, L., Lin, W., Mao, R.: Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. IEEE Trans. Parallel Distrib. Syst. **32**(7), 1539–1551 (2020)
14. Tian, Y., Wang, S., Xiong, J., Bi, R., Zhou, Z., Bhuiyan, M.Z.A.: Robust and privacy-preserving decentralized deep federated learning training: focusing on digital healthcare applications. In: IEEE/ACM Transactions on Computational Biology and Bioinformatics. https://doi.org/10.1109/TCBB.2023.3243932
15. Li, J., et al.: A federated learning based privacy-preserving smart healthcare system. IEEE Trans. Ind. Inform. **18**(3) (2021)
16. De Oliveira Fornasier, M.: The use of AI in digital health services and privacy regulation in GDPR and LGPD Between revolution and (dis)respect. RIL Brasília **59**(233), 201–220 (2022)
17. Zachariah, R., Ninh, A., Karnes, W.: Artificial intelligence for colon polyp detection: why should we embrace this? Tech. Innov. Gastrointestinal Endoscopy **22**(2), 48–51 (2020). https://doi.org/10.1016/j.tgie.2019.150631. https://www.sciencedirect.com/science/article/pii/S1096288319300701. ISSN 2590-0307
18. Huang, J., Jiang, Y.: Construction of gastroscope image recognition model and diagnosis system based on artificial intelligence technology. In: Proceedings of the SPIE 12703, Sixth International Conference on Intelligent Computing, Communication, and Devices (ICCD 2023), 127032E (2023). https://doi.org/10.1117/12.2682913
19. OECD.AI.OECD's live repository of AI strategies & policies
20. IQVIA. Digital Health Trends 2021. https://www.iqvia.com/insights/the-iqvia-institute/reports/digital-health-trends-2021. Accessed 24 June 2022
21. Kernebeck, S., Busse, T.S., Bottcher, M.D., Wetz, J., Ehlers, J., Bork, U.: Impact of mobile health and medical applications on clinical practice in gastroenterology. World J. Gastroentgerol. **26**(29), 4182–4197 (2020)
22. Desai, M., et al.: Use of smartphone applications to improve quality of bowel preparation for colonoscopy: a systematic review and metanalysis. Endosc. Int. Open (2019). 7Q E216-E224 [PMID 30705956]. https://doi.org/10.1067/mge.2003.294
23. OECD.AI (2021). https://oecd.ai/en/dashboards/overview
24. https://dhis2.org/in-action/#map. Accessed 07 Nov 2023
25. Hausenkamph, D.S., Cuadrado, D.C., Aarvik, P., Kirya, M.: U4 Issue 2022:9, Anti-corruption, transparency, and accountability in health management information systems, Chr. Michelsen Institute (CMI), Norway (2022)
26. Byrne, E., Sæbø, J.I.: Routine use of DHIS2 data: a scoping review. BMC Health Serv. Res. **22**, 1234 (2022). https://doi.org/10.1186/s12913-022-08598-8

27. Reynolds, E., et al.: Implementation of DHIS2 for disease surveillance in Guinea: 2015–2020. Front. Public Health **9**, 761196 (2022). https://doi.org/10.3389/fpubh.2021.761196
28. National Digital Health Strategy for South Africa 2019–2024, National Department of Health Republic of South Africa ISBN (digital) 978-1-920585-31-0. www.health.gov.za
29. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
30. Cybersecurity Incident Reporting and Analysis System (CIRAS). https://ciras.enisa.europa.eu/
31. ENISA "Threat Landscape:Health Sector – January 2021 to March 2023, p. 3 (2023)
32. Kazgan, M.: Real challenge in digital health entrepreneurship: changing the human behavior. In: Wulfovich, S., Meyers, A. (eds.) Digital Health Entrepreneurship. HI, pp. 7–15. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-12719-0_2
33. Iliadis, A.: Computer guts and swallowed sensors: ingestibles made palatable in an era of embodied computing. In: Pedersen, I., Iliadis, A. (eds.) Embodied Computing: Wearables, Embeddables, Ingestibles, pp. 1–20. The MIT Press, Cambridge (2020)
34. Gerke, S., Shachar, C., Chai, P.R., et al.: Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. Nat. Med. **26**, 1176–1182. https://doi.org/10.1038/s41591-020-0994-1(2020)
35. Grande, D., Luna Marti, X., Feuerstein-Simon, R., et al.: Health policy and privacy challenges associated with digital technology. JAMA New Open **3**(7), e208285 (2020). https://doi.org/10.1001/jamanetworkopen.2020.8285
36. Ali, A., et al.: Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics **10**, 2034 (2021). https://doi.org/10.3390/electronics10162034
37. Brost, G.S., Hoffmann, M.: Identifying security requirements and privacy concerns in digital health applications. In: Fricker, S.A., Thümmler, C., Gavras, A. (eds.) Requirements Engineering for Digital Health, pp. 133–154. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-09798-5_7
38. WHO. Resolution A71/20 on Digital Health (2018). https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_ACONF1-en.pdf. Accessed 19 July 2019
39. ITU-T FG-AI4H Deliverable Telecommunication Standardization Sector of ITU, DEL02 -Overview of regulatory concepts on artificial intelligence for health, DEL02 (2022)
40. Glenn, T., Monteith, S.: Privacy in the digital world: medical and health data outside the HIPAA protections. Curr. Psychiatry Rep. **16**(11), 494 (2014). https://doi.org/10.1007/s11920-014-0494-4
41. Hudson, K.L., Holohan, M.K., Collins, F.S.: Keeping pace with the times-the Genetic Information Nondiscrimination Act of 2008 N. Engl. J. Med. **358**(25), 2661–2663 (2008). https://doi.org/10.1056/NEJMp0803964
42. Bork, U., Weitz, Jr.: Cloud Computing im Gesundheitswesen: Mehr Chancen als Risiken, **116** (14), 679-screens (2019). Accessed 17 Feb 2020. Dtsch Arztebl International
43. Jain, D.: Regulation of digital healthcare in India: ethical and legal challenges. Healthcare [Internet] **11**(6), 911 (2023). https://doi.org/10.3390/healthcare11060911
44. Mint. Indian healthcare sector suffers 1.9 million cyberattacks in 2022. [Internet] (2022). Cited 11 Aug 2023. https://www.livemint.com/technology/tech-news/indian-healthcare-sector-suffers-1-9-million-cyberattacks-in-2022-11669878864152.htm

45. Ahmad, Z.: Al Meslamani Technical and regulatory challenges of digital health implementation in developing countries. J. Med. Econ. **26**(1), 1057–1060 (2023). https://doi.org/10.1080/13696998.2023.2249757
46. Yehualashet, D.E., Seboka, B.T., Tesfa, G.A., et al.: Barriers to the adoption of electronic medical record system in Ethiopia: a systematic review. J. Multidiscip. Healthc. **14**, 2597–2603 (2021). https://doi.org/10.2147/JMDH.S327539