Taylor & Francis
Taylor & Francis Group

Journal of Medical Economics

ISSN: (Print) (Online) Journal homepage: www.informahealthcare.com/journals/ijme20

Gaps in digital health policies: an insight into the current landscape

Ahmad Z. Al Meslamani

To cite this article: Ahmad Z. Al Meslamani (2023) Gaps in digital health policies: an insight into the current landscape, Journal of Medical Economics, 26:1, 1266-1268, DOI: 10.1080/13696998.2023.2266955

To link to this article: https://doi.org/10.1080/13696998.2023.2266955

Published online: 12 Oct 2023.

JOURNAL OF MEDICAL ECONOMICS
2023, VOL. 26, NO. 1, 1266–1268
https://doi.org/10.1080/13696998.2023.2266955
Article 0180-RT/2266955

Taylor & Francis
Taylor & Francis Group

EDITORIAL

Gaps in digital health policies: an insight into the current landscape

Introduction

Digital health (DH), defined as "*the use of information and communications technologies in medicine and other health professions to manage illnesses and health risks and to promote wellness*", has gained significant momentum due to its transformative potential[1]. DH encompasses technologies such as remote sensing and wearables for real-time health monitoring, telemedicine for remote consultations, and data analytics for predictive modelling. The field also includes health behaviour modification techniques, bioinformatics, medical social media, digital health records, patient-physician portals, decision support systems, and advanced imaging technologies[2].

Owing to the rapid expansion and diversification of DH technologies, comprehensive policies governing their use are crucial for ensuring safety, effectiveness, and equity. In this editorial, "safety" is interpreted predominantly from a legal standpoint, focusing on cyber threats and the legal implications of medical errors, rather than clinical safety. Health policies refer to the plans, decisions, and actions undertaken to achieve specific healthcare goals within a society, emphasizing the allocation and utilization of resources to improve health outcomes and accessibility[3]. In contrast, regulatory frameworks primarily pertain to the legal controls placed on digital health technologies to ensure safety, efficacy, and equitable access, encompassing issues of certification, reimbursement decisions, and access policies[3].

Drawing on the work of Greenhalgh et al. policies play a pivotal role in transitioning successful pilot projects to mainstream services. They help in identifying and addressing potential drivers or roadblocks at the policy level to prevent nonadoption or abandonment of services[4]. This perspective aligns with literature that underscores the importance of practical guidance for health system modernization, including funding reform and organizational changes in services[5].

Given the significant role that policies play in shaping the DH landscape, an in-depth evaluation of existing policies, their efficacy, and any existing gaps is critical. Understanding these aspects is essential for identifying opportunities for improvement and ensuring that implemented technologies maximize public health benefits while mitigating risks. This editorial aims to identify gaps and opportunities within existing DH policies, focusing on their impact on healthcare outcomes and equity.

Discussion

Gaps in digital health policies and regulations

The gaps in digital health policies and regulations are multifaceted, affecting the efficacy and sustainability of healthcare services (Table 1).

Regulatory lag

Regulatory lag, which describes a situation where the pace of technological advancement outstrips the rate of policy formulation. For examples, in India, the Telemedicine Practice Guidelines were only introduced in 2020, despite the widespread use of telemedicine services for over a decade, leading to various quality issues[6,7]. In the U.S., the Food and Drug Administration (FDA) has been criticized for its slow response to regulating mobile health applications[8]. During the recent COVID-19 pandemic, many countries, particularly those with low to middle incomes, have introduced telemedicine services. These services include online consultations, home delivery of medications, and remote prescription refills, often without the presence of national guidelines for telemedicine practice[9]. The absence of timely regulations affects the quality and safety of digital health applications. Many of these technologies operate in a "regulatory vacuum," where the lack of oversight can lead to ethical dilemmas, misuse, and even harm to patients. For healthcare providers, this creates a precarious situation where the adoption of new technologies comes with significant risk.

Data privacy

The concerns regarding data privacy have become increasingly prominent[10]. The World Health Organization has highlighted the substantial rise in health data collection, driven by the advent of wearable technologies, mobile health apps, and other digital platforms[11]. This proliferation of data sources has made the issue of data protection increasingly complex and urgent.

Globally, data privacy laws in digital health present a varied patchwork, each with its own degree of comprehensiveness and effectiveness[10]. The European Union's General Data Protection Regulation (GDPR) is widely recognized as the industry standard; however, it has limitations in geographical coverage and adaptability to emerging technologies like blockchain and AI[12]. The Health Insurance Portability and Accountability Act (HIPAA) in the U.S., while comprehensive, has been criticized for its complexity and for not covering newer digital health technologies, thus leaving a regulatory gap[13]. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is praised for its flexibility but, like HIPAA, struggles to keep pace with rapidly evolving digital health technologies[14]. China's recently enacted Personal Information Protection Law (PIPL) and Brazil's General Data Protection Law (LGPD), both inspired by GDPR, show promise but face challenges in implementation, particularly in safeguarding large volumes of health data and ensuring compliance in sensitive sectors like healthcare[14].

Table 1. Gaps in digital health (DH) regulations.

Gaps in DH regulations	Context	Implications
Regulatory Lag	Slow policy formulation	Reduced quality and safety of healthcare services
	absence of guidelines for new technologies like telemedicine	Ethical dilemmas
		Misuse of technology
		Increased risk for healthcare providers
		Potential for costly legal battles
Data privacy	Inadequate laws	Reduced public trust
	geographical limitations of existing laws	Hindrance to international research collaborations
		Potential for steep fines for healthcare providers
		Additional costs for damage control
Safety	Data security	Immediate and severe consequences for patient health
	Medical errors	Financial burdens due to potential lawsuits
		Reputational damage to healthcare providers.
Transparency	Data ownership	Biases
	Algorithmic bias,	Legal challenges related to user agreements
	Informed consent	Potential malpractice claims for incorrect diagnoses or treatment plans.
		Undermining of informed consent

Safety

Safety issues in digital health extend beyond data privacy and regulatory lag, directly impacting patient health. Generally, these concerns can be categorized into two main areas: data security and medical errors.

Existing regulations like HIPAA often prove inadequate in addressing evolving cyber threats. For instance, a recent data breach at Ascension's Texas hospitals potentially compromised the data of more than 18,000 patients[15].

Another critical safety concern is the risk of medical errors arising from software glitches or incorrect data input in various digital health systems like electronic prescribing systems or digital health records (DHRs). A study found that 34% of medication events in two U.S. intensive care units were related to DHRs. Medical errors related to electronic systems not only carried a greater risk of causing significant harm to patients but were also more commonly observed during the stage of medication ordering, as opposed to events not linked to electronic health records[16]

Transparency

Transparency remains a significant challenge in digital health, particularly in the areas of data ownership, algorithmic bias, and informed consent. Current regulations like HIPAA provide some guidance but fall short of fully elucidating the complexities of data ownership, especially when third-party tech companies are involved. For example, Google's Project Nightingale collected health data from millions of Americans in 2019 without explicit consent, sparking debates about data ownership[17].

Additionally, concerns exist about the lack of transparency in healthcare algorithms. A study showed that these algorithms were less likely to refer Black patients to specialized care programs, highlighting systemic biases[10]

As AI applications in imaging, diagnostics, and surgery become more prevalent, they introduce new challenges to the traditional patient-clinician relationship[10]. Questions arise about the extent to which clinicians should disclose information about the AI systems they use. This is particularly relevant for "black-box" algorithms like Corti's emergency dispatch system, which are not fully understood even by their developers[18].

Moreover, AI health apps and chatbots, increasingly used for services ranging from diet advice to medication adherence, add another layer of complexity to the informed consent landscape[19]. These apps often feature user agreements that most people neither fully read nor understand, raising ethical questions about what an ethically responsible user agreement should entail and how it should align with traditional informed consent documents.

Economic implications

The financial risks of failing to address these regulatory gaps are extremely high. They jeopardize not only patient safety and ethical standards but also the economic viability of healthcare providers and the industry as a whole. The potential costs associated with legal actions, fines, and reputational damage underscore the urgent need for comprehensive, adaptable policies that can keep pace with technological advancements in digital health.

Regulatory lag can lead to expensive legal battles and settlements if patients are harmed by unregulated or inadequately regulated technologies. Such legal costs can be financially crippling for healthcare providers, leading to increased insurance premiums and higher costs for healthcare services. A lack of trust in digital solutions due to these regulatory shortcomings could also slow adoption rates, pushing healthcare systems to revert to more costly traditional methods.

Data privacy concerns carry their own financial consequences. Breaches can result in substantial fines for healthcare providers, in addition to the costs incurred for damage control, such as public relations efforts and technological upgrades to prevent future incidents. Moreover, inconsistencies in privacy laws across countries can hinder global research collaborations, potentially delaying the development of cost-effective treatments.

Safety lapses, including data breaches and medical errors, can have catastrophic financial repercussions for healthcare providers. Beyond the immediate costs of remediation, providers may face multimillion-dollar lawsuits and legal fees. Such incidents can also damage a provider's reputation, affecting their business for years to come.

Transparency issues introduce another layer of financial complexity. The use of "black-box" algorithms in healthcare could lead to incorrect diagnoses or treatment plans, putting patient health at risk and exposing providers to malpractice

claims. Unclear user agreements for AI health apps and chatbots could also result in legal challenges, particularly if users believe their consent was not properly obtained.

Conclusion

The rapid emergence of digital health technologies offers both transformative opportunities and daunting challenges. Gaps in regulations related to data privacy, safety, and transparency pose serious threats to patient outcomes, ethical standards, and economic stability. These threats can manifest as potential legal battles, fines, and reputational damage to healthcare providers, as well as slow the adoption of new technologies. Given the urgency of these issues, it becomes increasingly essential to develop comprehensive, adaptable policies that can keep pace with the rapid changes occurring in the digital health technology landscape.

Transparency

Declaration of funding

The paper was not funded.

Declaration of financial/other relationships

The authors have no relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript. This includes employment, consultancies, honoraria, stock ownership or options, expert testimony, grants or patents received or pending, or royalties.

Author contributions

AZA did the study design development, data extraction, manuscript drafting and reviewing

Reviewer disclosures

Peer reviewers on this manuscript have no relevant financial or other relationships to disclose.

ORCID

Ahmad Z. Al Meslamani http://orcid.org/0000-0002-8370-9562

References

[1] Ronquillo Y, Meyers A, Korvek SJ. "Digital Health.," Treasure Island (FL),2023.
[2] Al Meslamani AZ, Kassem AB, El-Bassiouny NA, et al. An emergency plan for management of COVID-19 patients in rural areas. Int J Clin Pract. 2021;75(10):e14563. doi: 10.1111/ijcp.14563.
[3] Parajuli R, Bohara D, Kc M, et al. Challenges and opportunities for implementing digital health interventions in Nepal: a rapid review. Front Digit Heal. 2022;4:861019. doi: 10.3389/fdgth.2022.861019.
[4] Greenhalgh T, Wherton J, Papoutsi C, et al. Beyond adoption: a new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the Scale-Up, spread, and sustainability of health and care technologies. J Med Internet Res. 2017; 19(11):e367. doi: 10.2196/jmir.8775.
[5] Al Meslamani AZ, Aldulaymi R, El Sharu H, et al. The patterns and determinants of telemedicine use during the COVID-19 crisis: a nationwide study. J Am Pharm Assoc (2003). 2022;62(6):1778–1785. doi: 10.1016/j.japh.2022.05.020.
[6] Dinakaran D, Manjunatha N, Kumar CN, et al. Telemedicine practice guidelines of India, 2020: implications and challenges. Indian J Psychiatry. 2021;63(1):97–101. doi: 10.4103/psychiatry.IndianJPsychiatry_476_20.
[7] Al Meslamani AZ. Technical and regulatory challenges of digital health implementation in developing countries. J Med Econ. 2023;26(1):1057–1060. doi: 10.1080/13696998.2023.2249757.
[8] Larson RS. A path to Better-Quality mHealth apps. JMIR Mhealth Uhealth. 2018;6(7):e10414. doi: 10.2196/10414.
[9] Murshidi R, Hammouri M, Taha H, et al. Knowledge, attitudes, and perceptions of jordanians toward adopting and using telemedicine: national cross-sectional study. JMIR Hum Factors. 2022; 9(4):e41499. doi: 10.2196/41499.
[10] Gerke S, Minssen T, Cohen G. Chapter 12 - Ethical and legal challenges of artificial intelligence-driven healthcare. in Artificial intelligence in healthcare., A. Bohr and K. Memarzadeh, Eds., Academic Press, 2020, pp. 295–336. doi: 10.1016/B978-0-12-818438-7.00012-5.
[11] WHO. "Ethics and governance of artificial intelligence for health," 2021. [Online]. Available: https://www.who.int/publications/i/item/9789240029200.
[12] Li H, Yu L, He W. The impact of GDPR on global technology development. J Glob Inf Technol Manag. 2019;22(1):1–6. doi: 10.1080/1097198X.2019.1569186.
[13] Edemekong PF, Annamaraju P, Haydel MJ. "Health Insurance Portability and Accountability Act.," Treasure Island (FL),2023.
[14] Thorburn J. The personal information protection and electronic documents act and the protection of personal health information. Health Law Can. 2001;22(2):52–56.
[15] Beckr's Health IT, "18,000+ Ascension patients caught in data breach," 2023. https://www.beckershospitalreview.com/cybersecurity/18-000-ascension-patients-caught-in-data-breach.html. (accessed Aug. 31, 2023).
[16] Carayon P, Du S, Brown R, et al. EHR-related medication errors in two ICUs. J Healthc Risk Manag. 2017;36(3):6–15. doi: 10.1002/jhrm.21259.
[17] The Guardian. "Google's secret cache of medical data includes names and full details of millions – whistleblower," 2019. [Online]. Available: https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information.
[18] Vincent J. AI that detects cardiac arrests during emergency calls will be tested across Europe this summer. Verge. 2018; https://www.theverge.com/2018/4/25/17278994/ai-cardiac-arrest-corti-emergency-call-response (accessed Aug. 31, 2023).
[19] Al Meslamani AZ. Applications of AI in pharmacy practice: a look at hospital and community settings. J Med Econ. 2023;26(1): 1081–1084. doi: 10.1080/13696998.2023.2249758.

Ahmad Z. Al Meslamani
College of Pharmacy, Al Ain University, Abu Dhabi, United Arab Emirates;
AAU Health and Biomedical Research Center, Al Ain University, Abu Dhabi, United Arab Emirates
amaslamanie1095@gmail.com

Received 31 August 2023; revised 30 September 2023; accepted 2 October 2023