JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2026, 11(1), 299-305
ISSN: 2589-1316

Regulating Digital Health: Legal Perspectives on Medical ICT and Home Wellness Devices

Kafi Mahmud[1*], Mukesh Kumar[2], O.P. Midha[3]

[1] *Research Scholar, University Institute of Legal Studies, Chandigarh University Mohali, Punjab, India, Email: kafimahmud1@gmail.com, ORCID: https://orcid.org/0000-0002-2552-2433*
[2] *Assistant Pofessor, University Institute of Legal Studies, Chandigarh University Mohali, Punjab, India, Email: mukesh.e11381@cumail.in, ORCID: https://orcid.org/0009-0007-2286-292X*
[3] *Director, University Institute of Legal Studies, Chandigarh University Mohali, Punjab, India, Email: opmidha68@yahoo.com, ORCID: https://orcid.org/0009-0003-9086-0118*

*Corresponding Author: kafimahmud1@gmail.com

Citation: Mahmud, K., Kumar, M., & Midha, O. P. (2025). Regulating Digital Health: Legal Perspectives on Medical ICT and Home Wellness Devices, *Journal of Cultural Analysis and Social Change*, 11(1), 299-305. https://doi.org/10.64753/jcasc.v11i1.3674

Published: December 26, 2025

ABSTRACT

Medical Information and Communication Technologies (ICT) and Home Wellness devices that have proliferated are transforming healthcare delivery offering remote monitoring and personalized care. Yet such advancement also brings important regulatory challenges such as fragmented legal frameworks, privacy of data, device safety and liability issues. In this paper, the current legal regulation of Medical ICT and home wellness devices is studied and, with a focus on their regulatory gaps and difficulties in effective oversight, is researched. The first research questions address how these technologies are regulated by existing international and domestic legal frameworks and what legal issues are created when innovations are pitted against patient protection. Using a qualitative doctrinal methodology, the study carries out a systematic analysis of relevant statutes, regulations and judicial decisions to build a legal view of the issue. Scope includes medical devices subject to regulation by health authorities as well as wellness devices imagined at the crossroads of consumer technology and healthcare. Results illustrate regulatory approaches keeping up with the changes and inconsistences in regulatory approach, jurisdictional ambiguities and the necessity of further harmonization when dealing with new technological underpinnings. Finally, the study presents targeted legal reforms and an ongoing regulatory strategy, aimed at assuring patient safety, data security and accountability, while promoting innovation. The academic and practical discourse on digital health regulation is expanded by this research through a rigorous legal analysis that is critical for policymakers, regulators and stakeholders involved in the increasingly dynamic context of medical ICT and home wellness device governance.

Keywords: Digital Health, Legal Frameworks, Regulation, Medical ICT, Wellness Devices.

INTRODUCTION

In recent years, Medical Information and Communication Technologies (ICT) have come a long way as have Home Wellness devices have transformed the digital health ecosystem significantly. Limited to remote patient monitoring, personalized healthcare delivery and continuous wellness tracking, these technologies vastly improve both the accessibility of healthcare and patient engagement outside the traditional clinical setting [1]. Examples of medical ICT include telemedicine platforms, wearable biosensors, integrated health information systems, while home wellness devices are fitness trackers, smart thermometers and digital health apps that should be used by

consumers. Together they constitute a shift in the paradigm of healthcare away from centralized management toward a more decentralized approach where individuals are put in charge of their health [2].

While there are many benefits of these digital health tools, they are rapidly diffusing and the regulation and law of these tools are struggling to keep pace. But the sector's changing nature makes it difficult to set coherent legal frameworks addressing data privacy, device safety, liability and cross jurisdictional enforcement. The evolution of new modalities, functions and combinations of medical and consumer wellness functionalities, often merging with consumer technologies, challenges existing regulatory regimes which are often fragmented and developed on a region by region basis, to keep up [3]. While this regulatory ambiguity might decrease patient care security and data security, it leaves manufacturers and healthcare providers, as well as end users, in uncertainty [4]. Issues pertaining to key legal questions arise in regard to the adequacy of existing law to provide the necessary governing of ICT in medical and wellness devices, the delineation of regulatory responsibility and the mechanism that will ensure accountability in the digital health domain.

The article therefore seeks to critically analyze the legal frameworks that provide legal frameworks governing Medical ICT and home wellness devices which is essentially premised on the existing gaps and challenges and, subsequently, propose the potential routes for regulatory reform. The second research question in the study is (1) How do existing international and domestic legal systems regulate Medical ICT and home wellness devices? (2) How are these technologies currently being used bumps up against what legal and regulatory challenges stand in the way of effective oversight of these technologies? (3) What are the mechanisms by which legal frameworks can be adjusted to address needs and priorities of the industry, patients and those using the data?

The research is undertaken using qualitative doctrinal methodology, that is, looking at statutes, regulations and judicial decisions concerning digital health technologies. The present study focuses on the medical device regulatory spectrum as well as consumer wellness products business that straddles the line between healthcare and technology.

The present paper is organized as follows: Section II lists the literature for digital health regulation and legal aspects. Applicable laws and landmark case laws are examined in Section III. In Section IV is outlined the research methodology. Finally, findings and legal implications are discussed in Section V. Finally this section concludes the article with recommendations for future regulatory strategies and provides some concluding remarks.

LITERATURE REVIEW

Medical Information and Communication Technologies (ICT) and home wellness devices are important, ever evolving digital health technologies that have significant transformative impact on healthcare delivery and attract growing academic and regulatory attention on their regulation. Rapidly evolving, these technologies enable remote patient monitoring, personalized care and continuous wellness tracking and create a multitude of accompanying legal and regulatory issues.

Comprehensive overviews of digital health technologies are provided by recent studies which demonstrate how the use of Medical ICT technologies could advance clinical outcomes and patient empowerment but point to the fact that current regulatory frameworks do not suffice to address the dynamics and software orientation of Medical ICT. Innovations are often left behind and patient safety is threatened when regulatory systems for traditional medical devices are ill suited for keeping up with the latest developments. As a result, there is an urgent demand for regulation that is flexible with respect to technological advances[5], [6], [7].

Compounding matters is those datasets' jurisdictional and compliance issues, especially for telemedicine platforms and wearable health devices. Several current frameworks including those established by major regulatory authorities like the FDA and the European Medical Device Regulation are inadequate for the hybrid nature of wellness devices at the medical consumer product crossroads. As such, regulatory oversight is inconsistent and the proper management of cross border data flow and privacy protection is problematic [8], [9].

A regulatory 'grey zone' is also identified in terms of legal analyses of data protection laws applied to digital health devices. However, many such devices blur the conceptual lines between medical device and consumer product and as a result are difficult to enforce established data protection rules (e.g. HIPAA and GDPR). Third, this ambiguity risks patients privacy and leaves unclear to patients and manufacturers what responsibilities they should take in this issue [10], [11].

Central to this issue is cybersecurity, a still considerable regulatory gap, as current legal frameworks tend to be confined to general civil liability law and do not include specific instructions aimed at protecting sensitive health data from cyber threats. In particular, this deficiency is worrying, in view of the vulnerability of Medical ICT systems interconnected and calls for cybersecurity standards to be incorporated in the digital health governance [12], [13].

Additional challenges in software liability and accountability frameworks for software driven medical devices are also presented. The interactions between manufacturers, software developers and healthcare provider within digital health ecosystems are too complex to be dealt with efficiently by traditional product liability laws. However, the difficulty of attributing responsibility for software failures requires legal innovation to offer effective redress and protect the consumer from harm [14], [15], [16].

It is observed that International regulatory harmonization efforts have remained fragmented; variance in device classification, device approval process and post market surveillance is being observed across the jurisdictions. The fragmentation causes a hindrance for accessing the global market and is contradictive to patient safety, necessitating the reliance on the multilateral cooperation to harmonize different legal requirements and realize the unified oversight [17].

Collectively, these scholarly interventions reveal significant lacunae that now exist in legal research and regulatory practice around the relationship between medical device legislation, data protection, cybersecurity and liability in the case of home wellness devices. This thesis seeks to remedy these deficiencies by employing a qualitative doctrinal methodology that critically examines statutory instruments and judicial decisions to clarify the regulatory landscape and to suggest legal reform that would achieve a measure of balance between innovation, patient safety and patient privacy.

Existing Laws and Case Laws

Medical Information and Communication Technologies (ICT) and home wellness device regulation work within a multi-jurisdictional, multi regulatory regime. It looks at the key international and national laws, the enforcement regulatory authorities, landmark legal cases and legal structure's existing challenges.

Medical ICT, including home wellness products, are subject to a range of regulatory regimes created for the purpose of protecting against safety, efficacy and data protection dangers. Medical devices are regulated by U.S. Food and Drug Administration (FDA) under the Federal Food, Drug and Cosmetic Act (FDCA) and classified into three levels of risk (Class I, II and III) and most devices require pre-market clearance or approval [18]. The role of software driven health technologies is gaining in importance and in recent years the FDA has published specific guidance for Software as a Medical Device (SaMD) [19]. If so defined, this framework encompasses certain home wellness devices as well.

Specifically, since 2021, the European Union's Medical Device Regulation (MDR) which has applied to medical devices within EU member states, establishes a full legal regime related to medical devices. It stresses stricter conformity assessment procedures, more effective post market surveillance and more transparency. Some of the particular software provisions of the MDR represent an important indicator of the growing regulatory focus on software products [20].

Digital health governance is equally as critical, much so data privacy laws. Although not mental health related, the Health Insurance Portability and Accountability Act (HIPAA), 1996 in the U.S. sets standards that govern the privacy and security of patient health information; such standards, applied mainly to the providers, the insurers and their business associates [21]. But HIPAA doesn't quite extend so far when it comes to consumer wellness devices — many of which don't even fall under its thumb[22]. On the other hand, the European Union's General Data Protection Regulation (GDPR) provides greater coverage for digital health data by requiring the fulfillment of stringent data protection obligations of all entities processing personal data (including health related data) [23].

There's been a lot of attention given to digital health technologies and several agencies have key roles to play in overseeing them. The U.S. Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH) is the federal public health agency responsible for the regulation and evaluation of medical devices in the USA, including management of device risk and safety [24]. The MDR is supported for implementation by the European Medicines Agency (EMA) together with the control authorities of member states [25]. The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) enforces data privacy using HIPAA compliance, investigations over breaches [26]. In the EU, Data Protection Authorities (DPAs) pay for surveillance of firms to make sure they follow GDPR compliant and they have big assets to fine companies for violating GDPR.

Though the legal landscape of digital health has shifted more and more towards regulatory decisions, judicial decisions have often shaped that landscape. The U.S. case which is worth of note is Riegel v. A Medtronic, Inc. (2008) preempts certain state law claims for medical devices that are FDA approved premarket reducing manufacturer liability [27]. By making this decision, federal regulation wins out again but offers some uncertainty as to what options exist for consumers who are injured by device failure.

Multiple challenges are shown in the regulatory and judicial landscape. In the first place, the border between medical devices and consumer wellness products has become unclear, making regulation and law enforcement difficult. Many wellness devices with health related functionalities fall through (not strictly inside) the scope of medical device laws and there is regulatory gaps [28]. Second, the researchers explore the jurisdictional complexities raised by data privacy regulatory regimes for devices that collect sensitive health data and span legal jurisdictions.

The protections provided by GDPR are comprehensive, though enforcement of rules is inconsistent across jurisdictions and HIPAA applies only to consumer devices [29], [30]. Third, Riegel, based on the doctrine of preemption, severely limits state level legal remedies for harms resulting from devices and thus cuts off manufacturer liability [27]. The problem of liability for alleged defects has been compounded by a fragmented approach to liability in software driven devices. Finally technological evolution is outpacing regulatory adaptation. The most common cybersecurity related issues include lack of specific laws dealing with cybersecurity risks, lack of legislation for interoperability with digital health devices and artificial intelligence integrations [31].

Thus, existing international and national legal frameworks serve as foundation for Medical ICT and home wellness devices, but there is nevertheless large room for and the need to, improve. They paint a broader picture, involving other landmarks cases, of the tensions between authority of regulators, data protection and liability. Starting to meet these challenges necessitates a coordinated set of legal reforms and harmonized regulatory strategies designed to enable advances in technology while providing patient safety and privacy.

METHODOLOGY

The present research utilizes a qualitative doctrinal legal research design suitable for the thoughtful and rigorous analysis of Medical Information and Communication Technologies (ICT) and home wellness devices as legal principles and regulatory frameworks. The doctrinal methodology provides the means for a carefully developed interpretive analysis of these statutory, regulatory and judicial instruments, to arrive at a critical understanding of the normative digital health technology legal landscape. Authoritative legal texts are important primary data sources; comprising international treaties, national statutes and regulations. Moreover, principles in the application of legal standards and judicial reasoning of seminal case law related to Medical ICT and home wellness devices are analyzed to understand their practical application.

From a doctrinal analytical framework, regulatory gaps, inconsistencies and emerging challenges are identified through systematic synthesis of legal provisions and case precedents. This is supplemented with a comparative legal approach that compares regulatory regimes in other jurisdictions, including the United States and the European Union, in order to trace out patterns of both convergence and divergence in governance models.

Despite its strengths, the present research recognizes the limitations of a doctrinal inquiry – its ability to represent the dynamic socio technical effects of rapidly changing technologies is quite restrictive. In addition, findings are limited by a lack of available empirical data and a predominance of regulatory focus on certain jurisdictions.

FINDINGS AND DISCUSSION

The research synthesizes its results from the literature review, doctrinal analysis of relevant laws and case law to answer research questions about the regulation of Medical Information and Communication Technologies (ICT) and home wellness devices. Key legal challenges are analyzed, current regulatory frameworks evaluated and emerging trends for future legal governance are explored.

Regulation of Medical ICT and home wellness devices is a fragmented one and continuously evolving. Current U.S. FDA medical device regulations, European Union's Medical Device Regulation (MDR), HIPAA and GDPR constitute initial protections covering device safety, effectiveness and personal data security. Yet, legal categorizations of traditional divisions of medical and consumer wellness devices remain difficult in the face of the rapid convergence of medical and consumer wellness device technology. For one, many home wellness devices combine the traits of traditional and medical devices (e.g. hybrid devices) which sit outside of the full purview of strict medical device regulations that nonetheless implicate protected health data protected under privacy laws.

The primary results of the present analysis include regulatory uncertainty, data protection vulnerabilities and liability uncertainties. Inconsistencies between the classification criteria across different jurisdictions, as well as the fuzziness between regulated medical devices and wellness products create regulatory ambiguity. This ambiguity then makes compliance efforts and enforcement more difficult and could permit certain higher risk devices escape more rigorous scrutiny. Another one of the critical challenge is data protection. Despite the high standard achieved by GDPR for health data privacy in Europe, gaps exist in applying the same standards to consumer wellness devices, outside of very stringent healthcare settings. HIPAA's extremely limited scope with respect to consumer devices uncovered significant consumer related health data that is at serious risk of misuse or breach. These risks are compounded by cybersecurity deficiencies because current legal frameworks fall short of requiring comprehensive security controls for the Medical ICT systems which leave systems open to threat that could jeopardize patient safety.

Liability issues are very prominent too. The challenges of the diffused software driven digital health ecosystem create issues wherein traditional product liability doctrines are unable to accommodate the responsibility of manufacturers, software developers and healthcare providers. Preemption doctrines that shield manufacturers are shown to be at odds with the requisite need to hold companies accountable when device malfunction or provide inaccurate data.

Although existing laws have played a huge part in setting minimum safety and privacy standards, the current regulatory environment is too inflexible to adapt quickly to the pace of innovation. Currently, regulatory frameworks emphasize discrete features such as device safety, data privacy or market approvals, without integrating these features into a governing framework that would be appropriate for the multi–dimensional digital health technologies. Currently, there are no harmonized global standards which prevent streamlined regulatory approval and post market surveillance, consequently incurring higher compliance costs and lower legal clarity.

Furthermore, the enforcement mechanisms related with data privacy breaches and cybersecurity breaches are non existent or inconsistent and reactive rather than preventive. Existing legal instruments fail to capture these emerging issues that touch many Medical ICT and wellness devices, including artificial intelligence integration, interoperability and real-time data analytics.

Several trends point towards directions in which legal frameworks are evolving. The need for international level regulatory harmonization is increasingly being recognized in order to foster innovation ensures user safety. Streamlining of classification systems, approval processes and post market surveillance through the collaborative regulatory initiatives would create a more predictable legal environment.

In recent guidance documents for example, it has been recommended that such obligations should be integrated into device regulation through cybersecurity mandates to thereby integrate security-by-design principles and continuous monitoring. Emerging technologies such as artificial intelligence, also warrant regulatory approaches that are also adaptive, with regard to algorithmic transparency, bias and accountability.

Additionally, more comprehensive data governance concepts, going beyond simply privacy, are being subsumed under legal frameworks such as data portability, consent management and ethical utilization of heath data. An important premise to reconcile technological advancement and fundamental rights and patient trust, is this holistic perspective.

The research supports that the structures of foundation for regulatory of Medical ICT and home wellness devices, while exist, have challenges. The present study stresses the imperative to develop harmonized, adaptive legal frameworks that highlights device safety, data protection, liability and other emerging technological risks. Fulfillment of the dual imperatives of promoting innovation and assuring strong consumer protection in the developing digital health ecosystem therefore requires addressing these shortcomings.

CONCLUSION

The present study investigated qualitatively the regulatory landscape of Medical ICT and home wellness devices. The inferable outcomes of the analysis found that existing legal frameworks such as FDA regulations, the MDR, HIPAA and GDPR offer a foundation of piecemeal protections on device safety, data privacy and liability. The ambiguity of the regulation is, however, not yet solved, especially when hybrid devices straddle medical and consumer wellness categories. The result is considerable challenging in effective governance, compliance and enforcement, amplified by jurisdictional disparity and scant harmonization.

Persistent risks surrounding data protection vulnerabilities, cybersecurity gaps and liability issues of software driven digital health ecosystems are highlighted in some key findings. A particularly thorny thread has emerged in these cases between regulatory preemption and consumer accountability, emblemized in landmark case law. In addition, existing frameworks are not scalable to emerging technologies including artificial intelligence and the interconnected health systems, necessitating an adaptive regulatory evolution.

These findings have policy implications for the need for policymakers to develop harmonized, technology sensitive legal frameworks that address comprehensively device safety, privacy and liability. To avoid legal risks, manufacturers should make compliance with changing standards such as cybersecurity and data governance, their top priority. Healthcare providers, however, would be well advised to keep an eye on regulatory developments in the area so they can implement safe and lawful use of digital health tools in delivering care.

We call for future research to empirically evaluate the impacts of these regulatory reforms as well as to explore interdisciplinary approaches to studying the socio technical aspects of digital health. To achieve the advancement of international cooperation, device classification and to embed adaptive mechanisms to accommodate snappy innovative technology, legal reforms must protect the patient rights, but create an environment conducive to innovation.

REFERENCES

[1] A. I. Stoumpos, F. Kitsios, and M. A. Talias, "Digital Transformation in Healthcare: Technology Acceptance and Its Applications," Int J Environ Res Public Health, vol. 20, no. 4, p. 3407, Feb. 2023, doi: 10.3390/ijerph20043407.

[2] S. B. Junaid et al., "Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey," Healthcare (Basel), vol. 10, no. 10, p. 1940, Oct. 2022, doi: 10.3390/healthcare10101940.

[3] J. Torous, A. D. Stern, and F. T. Bourgeois, "Regulatory considerations to keep pace with innovation in digital health products," NPJ Digit Med, vol. 5, p. 121, Aug. 2022, doi: 10.1038/s41746-022-00668-9.

[4] A.-M. Howell, E. M. Burns, G. Bouras, L. J. Donaldson, T. Athanasiou, and A. Darzi, "Can Patient Safety Incident Reports Be Used to Compare Hospital Safety? Results from a Quantitative Analysis of the English National Reporting and Learning System Data," PLoS One, vol. 10, no. 12, p. e0144107, 2015, doi: 10.1371/journal.pone.0144107.

[5] T. Risling, J. Martinez, J. Young, and N. Thorp-Froslie, "Defining Empowerment and Supporting Engagement Using Patient Views From the Citizen Health Information Portal: Qualitative Study," JMIR Medical Informatics, vol. 6, no. 3, p. e8828, Sep. 2018, doi: 10.2196/medinform.8828.

[6] L. Karni, K. Dalal, M. Memedi, D. Kalra, and G. O. Klein, "Information and Communications Technology–Based Interventions Targeting Patient Empowerment: Framework Development," Journal of Medical Internet Research, vol. 22, no. 8, p. e17459, Aug. 2020, doi: 10.2196/17459.

[7] V. Petit-Steeghs, C. A. Pittens, J. Oosterman, and J. E. Broerse, "Co-creating an empowering health education intervention for urological cancer patients," Health Education Journal, vol. 80, no. 8, pp. 948–960, Dec. 2021, doi: 10.1177/00178969211035169.

[8] M. Słok-Wódkowska and J. Mazur, "Between commodification and data protection: Regulatory models governing cross-border information transfers in regional trade agreements," Leiden Journal of International Law, vol. 37, no. 1, pp. 111–138, Mar. 2024, doi: 10.1017/S092215652300050X.

[9] L. Lu et al., "Wearable Health Devices in Health Care: Narrative Systematic Review," JMIR mHealth and uHealth, vol. 8, no. 11, p. e18907, Nov. 2020, doi: 10.2196/18907.

[10] L. Marelli, Lievevrouw ,Elisa, and I. and Van Hoyweghen, "Fit for purpose? The GDPR and the governance of European digital health," Policy Studies, vol. 41, no. 5, pp. 447–467, Sep. 2020, doi: 10.1080/01442872.2020.1724929.

[11] B. Yuan and J. Li, "The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation," International Journal of Environmental Research and Public Health, vol. 16, no. 6, Art. no. 6, Jan. 2019, doi: 10.3390/ijerph16061070.

[12] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.

[13] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health Care and Cybersecurity: Bibliometric Analysis of the Literature," Journal of Medical Internet Research, vol. 21, no. 2, p. e12644, Feb. 2019, doi: 10.2196/12644.

[14] K. Drabiak, "Leveraging law and ethics to promote safe and reliable AI/ML in healthcare," Front. Nucl. Med., vol. 2, Sep. 2022, doi: 10.3389/fnume.2022.983340.

[15] G. Maliha, S. Gerke, I. G. Cohen, and R. B. Parikh, "Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation," The Milbank Quarterly, vol. 99, no. 3, pp. 629–647, 2021, doi: 10.1111/1468-0009.12504.

[16] H. Smith and K. Fotheringham, "Artificial intelligence in clinical decision-making: Rethinking liability," Medical Law International, vol. 20, no. 2, pp. 131–154, Jun. 2020, doi: 10.1177/0968533220945766.

[17] S. Alqahtani, E. Seoane-Vazquez, R. Rodriguez-Monguio, and T. Eguale, "Priority review drugs approved by the FDA and the EMA: time for international regulatory harmonization of pharmaceuticals?," Pharmacoepidemiology and Drug Safety, vol. 24, no. 7, pp. 709–715, 2015, doi: 10.1002/pds.3793.

[18] J. J. Darrow, J. Avorn, and A. S. Kesselheim, "FDA Regulation and Approval of Medical Devices: 1976-2020," JAMA, vol. 326, no. 5, pp. 420–432, Aug. 2021, doi: 10.1001/jama.2021.11171.

[19] M. R. Moshi, J. Parsons, R. Tooher, and T. Merlin, "Evaluation of Mobile Health Applications: Is Regulatory Policy Up to the Challenge?," International Journal of Technology Assessment in Health Care, vol. 35, no. 4, pp. 351–360, Jan. 2019, doi: 10.1017/S0266462319000461.

[20] B. Kearney and O. McDermott, "The Challenges for Manufacturers of the Increased Clinical Evaluation in the European Medical Device Regulations: A Quantitative Study," Ther Innov Regul Sci, vol. 57, no. 4, pp. 783–796, Jul. 2023, doi: 10.1007/s43441-023-00527-z.

[21] M. Alsaadi, M. Qasaimeh, S. Tedmori, and K. Almakadmeh, "HIPAA Security and Privacy Rules Auditing in Extreme Programming Environments," International Journal of Information Systems in the Service Sector

(IJISSS), vol. 9, no. 1, pp. 1–21, 2017, doi: 10.4018/IJISSS.2017010101.
[22] S. Feng, M. Mäntymäki, A. Dhir, and H. Salmela, "How Self-tracking and the Quantified Self Promote Health and Well-being: Systematic Review," Journal of Medical Internet Research, vol. 23, no. 9, p. e25171, Sep. 2021, doi: 10.2196/25171.
[23] R. Hussein et al., "General Data Protection Regulation (GDPR) Toolkit for Digital Health," in MEDINFO 2021: One World, One Health – Global Partnership for Digital Innovation, IOS Press, 2022, pp. 222–226. doi: 10.3233/SHTI220066.
[24] R. Khirasaria, V. Singh, and A. Batta, "Exploring digital therapeutics: The next paradigm of modern health-care industry," Perspectives in Clinical Research, vol. 11, no. 2, p. 54, Jun. 2020, doi: 10.4103/picr.PICR_89_19.
[25] L. Keutzer and U. S. Simonsson, "Medical Device Apps: An Introduction to Regulatory Affairs for Developers," JMIR mHealth and uHealth, vol. 8, no. 6, p. e17567, Jun. 2020, doi: 10.2196/17567.
[26] N. Yaraghi and R. D. Gopal, "The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study," The Milbank Quarterly, vol. 96, no. 1, pp. 144–166, 2018, doi: 10.1111/1468-0009.12314.
[27] "Riegel v. Medtronic, Inc., 552 U.S. 312 (2008)," Justia Law. Accessed: May 23, 2025. [Online]. Available: https://supreme.justia.com/cases/federal/us/552/312/
[28] S. Awad, L. Aljuburi, R. S. Lumsden, M. Mpandzou, and R. Marinus, "Connected health in US, EU, and China: opportunities to accelerate regulation of connected health technologies to optimize their role in medicines development," Front. Med., vol. 10, Aug. 2023, doi: 10.3389/fmed.2023.1248912.
[29] M. Cao et al., "Developing remote patient monitoring infrastructure using commercially available cloud platforms," Front. Digit. Health, vol. 6, Nov. 2024, doi: 10.3389/fdgth.2024.1399461.
[30] B. J. Evans, "The Perils of Parity: Should Citizen Science and Traditional Research Follow the Same Ethical and Privacy Principles?," Journal of Law, Medicine & Ethics, vol. 48, no. S1, pp. 74–81, Apr. 2020, doi: 10.1177/1073110520917031.
[31] S. Gilbert, M. Fenech, M. Hirsch, S. Upadhyay, A. Biasiucci, and J. Starlinger, "Algorithm Change Protocols in the Regulation of Adaptive Machine Learning–Based Medical Devices," Journal of Medical Internet Research, vol. 23, no. 10, p. e30545, Oct. 2021, doi: 10.2196/30545.

