*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


# BRIDGING THE REGULATORY DIVIDE: ENSURING SAFETY AND EQUITY IN WEARABLE HEALTH TECHNOLOGIES

Toshmatova Visolakhon Ikrom kizi
Doctor of Philosophy in Law (PhD), Lecturer, Department of International Law and Public Law Disciplines, University of World Economy and Diplomacy
Email: visolka1202@gmail.com

**Abstract**
Wearable medical devices are becoming common tools for health monitoring and therapy, offering personalized and preventive care. However, their rapid growth outpaces legal regulation, creating a gap that threatens patient safety and equity in healthcare. This article examines international regulatory approaches, key issues of safety and data protection, and the accessibility of such technologies for different population groups. Successful regulatory examples illustrate effective strategies for safeguarding user rights. The conclusion stresses a balanced approach: strict oversight of safety and privacy while fostering innovation and ensuring equal access to wearable medical technologies.

**Keywords:** Wearable medical devices; regulation; safety; privacy; equity; accessibility; health data.

## Introduction

Modern wearable devices for continuous monitoring of physiological indicators are expanding the possibilities of clinical practice and personal health management. These include fitness trackers, smartwatches with ECG functions, portable glucose monitors, and other gadgets that aid in early diagnosis and observation. Their spread is closely tied to the digitalization of healthcare and the rise of telemedicine, a trend that became especially evident during the COVID-

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


19 pandemic.[1] However, the development of legal and ethical standards has lagged behind technological progress, creating a regulatory gap—existing oversight mechanisms do not yet cover the new risks and specific features of wearable medical devices.[2]

Key risks associated with this regulatory gap include the safety of the devices themselves—sensor accuracy, algorithm reliability, and protection of confidential health data—as well as ethical challenges, such as ensuring equity and avoiding technological inequality. [3] The rapid adoption of wearables is already accompanied by technical, legal, and ethical issues, ranging from battery quality and sensor calibration to global legal dilemmas.[4]

Without an adequate regulatory framework, the promised benefits—improved treatment outcomes, disease prevention, and broader access to healthcare—may be undermined by a loss of user trust or the emergence of new forms of health inequity[5]

## Main Section

In the United States, the Food and Drug Administration (FDA) applies a risk-based approach: any device with diagnostic or therapeutic functions requires FDA clearance or approval, while general wellness gadgets (for example, fitness trackers) do not need formal certification. If a medical function is claimed—as with the ECG feature in the Apple Watch—evidence of safety and effectiveness is mandatory. In 2018, the FDA rapidly authorized this function, confirming its readiness to integrate innovations quickly while maintaining safety requirements[6].

[1] World Health Organization. WHO guideline: Recommendations on digital interventions for health system strengthening. Geneva: WHO, 2019. Available at: https://www.who.int/publications/i/item/9789241550505
[2] European Commission. Regulation (EU) 2017/745 on medical devices (MDR). Official Journal of the European Union, 2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745
[3] Bouderhem R. Privacy and regulatory issues in wearable health technology. Engineering Proceedings, 2023, 58(1):87. DOI: 10.3390/ecsa-10-16206
[4]U.S. Food and Drug Administration. Digital Health Center of Excellence—Wearables and Health. FDA, updated 2024. Available at: https://www.fda.gov/medical-devices/digital-health-center-excellence
[5] Robeznieks A. Wearables, the FDA and patient advice: What physicians should know. American Medical Association, 2019. URL: https://www.ama-assn.org/practice-management/digital-health/wearables-fda-and-patient-advice-what-physicians-should-know
[6] U.S. Food and Drug Administration. Apple Watch ECG App Clearance. FDA, 2018. Available at: https://www.fda.gov/medical-devices/digital-health-center-excellence

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


Alongside device oversight, the Health Insurance Portability and Accountability Act (HIPAA) establishes strict rules for the confidentiality and protection of protected health information (PHI), including data from physician-prescribed wearable sensors[7]. However, HIPAA does not cover all consumer devices used without a physician's involvement, so data collected by popular fitness trackers often fall outside the scope of the law. This highlights the need to update the regulatory framework as consumer gadgets increasingly overlap with medical functions.

Looking ahead, U.S. regulators may extend safety requirements to such devices if they continue to be marketed as medical tools. In addition, the FDA is preparing new guidance documents and "regulatory sandboxes" for digital health technologies to address the growing number of wearable medical devices[8].

The European Union applies a comprehensive approach to regulating wearable devices. The General Data Protection Regulation (GDPR), in force since 2018, sets high standards of privacy and cybersecurity for personal data, including health information, and imposes significant penalties for non-compliance. [9]

For the devices themselves, EU Regulation 2017/745 on Medical Devices (MDR), effective from 2021, broadened the definition of a medical device: smart wearables with diagnostic or therapeutic functions now require CE certification and an independent assessment of safety and effectiveness by notified bodies.[10]

In 2023, the EU adopted the Data Act, which establishes rules for fair access to information generated by electronic devices, including wearable medical sensors. Its purpose is to secure users' rights to their data and ensure transparent data use, complementing GDPR and closing existing legal gaps.[11]

[7] U.S. Department of Health & Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Available at: https://www.hhs.gov/hipaa/index.html
[8] Bouderhem R. Privacy and regulatory issues in wearable health technology. Engineering Proceedings, 2023. DOI: 10.3390/ecsa-10-16206
[9] European Parliament and Council. General Data Protection Regulation (EU) 2016/679. 2018. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[10] European Parliament and Council. Regulation (EU) 2017/745 on Medical Devices (MDR). 2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745
[11] European Commission. Proposal and political agreement on the Data Act. 2023. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-act

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


Regarding standardization, there is no single regulation specifically for "smart wearables." Instead, manufacturers must define the intended purpose of the product and comply with all relevant directives—radiofrequency, electrical, medical, and others. The universal mark of compliance, the CE label, confirms that these requirements are met.

Many countries adopt the experience of leading regulators or develop their own models of oversight. In the United Kingdom, the Medicines and Healthcare products Regulatory Agency (MHRA) oversees medical technologies, publishes guidance on digital health, and requires the registration of applications and wearable devices with medical functions. [12]In China, such gadgets are certified by the National Medical Products Administration (NMPA) and are subject to laws on cybersecurity and personal data protection.[13] Across parts of Asia and the Middle East—for example, in Singapore, Israel, and the United Arab Emirates—national digital health strategies set specific standards for telemedicine devices and mobile health applications. The overall trend is to find a balance between flexibility for innovation and patient safety.

At the international level, the World Health Organization (WHO) plays an increasingly active role, issuing recommendations on the standardization of medical technologies, including wearable devices. WHO experts emphasize the need for global coordination on ethical data use, cross-manufacturer device compatibility, and the protection of patient rights.

The widespread deployment of wearable medical devices has exposed serious issues of information security and privacy. Health-related personal data are highly sensitive and require special protection. However, continuous transmission of information via wireless networks and cloud services creates risks of leaks and unauthorized access.[14]

[12] UK Medicines and Healthcare products Regulatory Agency. Guidance on digital health, including medical device software and apps. Available at: https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency

[13] National Medical Products Administration of China. Regulations on medical device supervision and cybersecurity. Available at: https://www.nmpa.gov.cn

[14] Ministry of Health Singapore; Israeli Ministry of Health; UAE Ministry of Health. National digital health strategies, 2020–2024

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


The key challenge is ensuring confidentiality as the volume and value of collected medical information grow. Major threats involve cyberattacks and the human factor: staff or user errors, incorrect cloud configuration, or failure to follow security protocols. Experts recommend regular risk assessments and employee training, as well as strict access policies with multifactor authentication and role-based permissions.[15] Additional safeguards include encryption and the use of VPNs when transmitting data.[16] Thus, cybersecurity must become an integral part of wearable medical system infrastructure, on par with clinical effectiveness.

An important aspect is data transparency and user control. Many users are unaware of what information their devices collect or who has access to it. The principle of transparency, enshrined in the European Union's General Data Protection Regulation (GDPR), requires companies to provide a clear privacy policy and obtain informed consent so that individuals maintain control of their information even after it is shared with a physician or an application.[17]

In practice, this means the right to view, export, and delete personal data, as well as to be notified of every instance of its use. However, developers often fail to follow these principles. The high commercial value of health data creates a risk of misuse—for example, for marketing purposes or for sale to insurance companies.[18]

International norms—such as the GDPR in the EU and the U.S. Federal Trade Commission (FTC) guidelines—require data minimization and restrict use strictly to declared purposes.

At the national level, new laws are emerging: the United States has enacted a federal act regulating digital medical data outside the scope of HIPAA, and several states (including California and New York) have adopted their own

[15] Canali S., Schiaffonati V., Aliverti A. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. PLOS Digital Health, 2022. DOI: 10.1371/journal.pdig.0000104
[16] U.S. National Institute of Standards and Technology (NIST). Guide to VPN Security. Special Publication 800-77, Rev.1, 2021. Available at: https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final
[17] European Parliament and Council. General Data Protection Regulation (EU) 2016/679. 2018. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[18] Bouderhem R. Privacy and regulatory issues in wearable health technology. Engineering Proceedings, 2023, 58(1):87. DOI: 10.3390/ecsa-10-16206

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


biometric information laws. In the European Union, the upcoming Data Act is expected to strengthen user rights and complement the GDPR.[19]

Ensuring the security of wearable medical devices presents serious challenges. These include the reliability of device software and its resistance to failures. If a device provides inaccurate readings—for example, heart-rate monitors on smart bands may give erroneous results under certain wearing conditions—this can lead to incorrect decisions by the user or a physician. Therefore, accuracy and data quality are not only technical but also regulatory issues: manufacturers must confirm the clinical validity of their algorithms. Regulators in several countries require companies to provide evidence of measurement quality through clinical trials or ISO certification for biomedical sensors (e.g., ISO 80601-2-61 for pulse oximeters).[20]

Regular firmware updates are often intended to eliminate security vulnerabilities. These updates must be delivered to users in a timely manner; otherwise, a device running outdated software becomes a weak link in the overall security system[21].

Guaranteeing the safety and confidentiality of wearable health technologies requires a comprehensive approach that combines:

- ❖ Technical measures—encryption, robust cybersecurity practices, and high-precision sensors;
- ❖ Organizational policies—strict access controls, regular audits, and staff/user training;
- ❖ Legal guarantees—strong data-protection laws, international standards, and enforceable penalties for violations.[22]

Only such an integrated strategy can create the level of trust necessary for widespread adoption; a single major data leak or security incident could seriously undermine public confidence.

Moreover, new technologies initially reach wealthier and more technologically literate groups, exacerbating the digital divide. Younger and more affluent users

[19] California Consumer Privacy Act (CCPA), 2018; New York Privacy Act, 2021.
[20] International Organization for Standardization. ISO 80601-2-61: Particular requirements for pulse oximeter equipment. Geneva: ISO, 2017
[21] U.S. Food and Drug Administration. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. FDA, 2023. Available at: https://www.fda.gov
[22] European Commission. General Data Protection Regulation (EU) 2016/679; Proposal on the Data Act, 2023

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


are far more likely to use fitness trackers, while older adults and rural residents face financial barriers, low digital literacy, and insufficient internet infrastructure, reducing their access to wearable innovations[23].

Insufficient data representativeness leads to algorithms and sensors performing less accurately for certain ethnic and demographic groups, as confirmed by research on bias in AI systems.[24]

Strategies to address this include:

- Subsidies and insurance coverage for devices,
- Digital literacy programs,
- Inclusive design—taking into account the needs of diverse user groups during development. An example is the use of flexible wireless sensors successfully deployed in clinics across Africa and Asia, which demonstrate the benefits of inclusive engineering.[25]

When properly integrated, wearable technologies help reduce inequality: telemedicine and remote monitoring improve access to physicians in remote regions, as shown by pilot projects in India and several African countries. For regulators, key priorities include standardization and device interoperability, as well as evaluating whether these technologies reduce—or unintentionally widen—health disparities between population groups.[26]

Despite these challenges, several countries have already implemented effective regulatory mechanisms for wearable medical devices:

- European Union (EU): The General Data Protection Regulation (GDPR, 2018) set a global benchmark for data protection, forcing manufacturers to strengthen privacy practices. In addition, the Medical Device Regulation (MDR)

[23] Zinzuwadia S., Singh P. Digital inequality in wearable health technologies. Journal of Global Health, 2022. DOI: 10.7189/jogh.12.04067
[24] Zinzuwadia S., Singh P. Digital inequality and algorithmic bias in wearable health technologies. Journal of Global Health, 2022. DOI: 10.7189/jogh.12.04067
[25] Walter A., et al. Patient-centered engineering of flexible wireless sensors for low-resource settings. Nature Medicine, 2024. DOI: 10.1038/s41591-024-03210-3
[26] World Intellectual Property Organization (WIPO). Telemedicine and remote monitoring initiatives in India and Africa. 2023. Available at: https://www.wipo.int

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


enhanced quality control of medical devices, including wearables, through mandatory CE certification.[27]

❖ United States (US): The Food and Drug Administration (FDA) employs flexible regulatory pathways—programs such as the Pre-Cert Program and the Digital Health Center of Excellence accelerate the market entry of innovations while maintaining safety requirements. FDA's approval of the ECG feature in the Apple Watch and its Emergency Use Authorizations (EUAs) for remote monitoring devices during COVID-19 demonstrated the regulator's ability to respond rapidly while safeguarding public health.[28]

**United Kingdom (UK):** The **National Health Service (NHS)** evaluates digital health solutions under the **Digital Health Technology Standard**, while the **Medicines and Healthcare products Regulatory Agency (MHRA)** publishes clear regulatory guidance. This framework enabled the integration of the portable **KardiaMobile ECG patch** into general practitioners' clinical practice.[29]

**Germany:** The **DiGA program** grants physicians the right to prescribe **certified digital health applications** with **health insurance coverage**, creating a model for integrating software and wearable sensors into standard treatment protocols.[30]

**Industry Self-Regulation:** Major manufacturers have developed their own **codes of fair data use** and **data-exchange standards**, such as the **IEEE interoperability initiative**, simplifying device compatibility and increasing public trust in wearable technologies.[31]

These examples demonstrate that a combination of **strict regulations**, **flexible procedures**, and **industry-led initiatives** can ensure both **safety** and **innovation** in the deployment of wearable medical devices.

[27] European Parliament and Council. General Data Protection Regulation (EU) 2016/679, 2018; Regulation (EU) 2017/745 on Medical Devices. Available at: https://eur-lex.europa.eu

[28] U.S. Food and Drug Administration. Emergency Use Authorizations for remote patient monitoring devices during COVID-19. 2020. Available at: https://www.fda.gov/emergency-preparedness-and-response/mcm-legal-regulatory-and-policy-framework/emergency-use-authorization

[29] UK National Health Service. Digital Technology Assessment Criteria (DTAC) and Digital Health Technology Standard. Available at: https://www.nhsx.nhs.uk/digital-technology-assessment-criteria-dtac

[30] Federal Institute for Drugs and Medical Devices (BfArM). Digital Health Applications (DiGA) Directory. Available at: https://diga.bfarm.de/de/verzeichnis

[31] IEEE Standards Association. IEEE P360 – Wearable Device Interoperability Initiative. Available at: https://standards.ieee.org

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


The regulatory gap in the field of wearable medical technologies persists but is gradually narrowing thanks to the joint actions of regulators and industry. An international analysis highlights several key areas for progress:

- Data Quality. National and international standards for measurement accuracy and clinical validation of devices are essential. Certification under ISO/IEC standards and the quality-by-design principle—embedding reliability at the design stage—are strongly recommended.[32]
- Interoperability. To integrate data from different devices, compatibility with medical information systems and unified data-exchange protocols such as HL7, IEEE, and FHIR are required. Regulators should actively encourage their adoption.[33]
- Cybersecurity and Privacy. Mandating encryption, multifactor authentication, regular audits, and transparent data-use policies is critical. Users must have a full understanding of who accesses their data and how it is used.[34]
- Equitable Access. Regulation must account for social justice: supporting affordable devices, excluding substandard products, enforcing accessibility standards for the elderly and persons with disabilities, and introducing subsidy programs to reduce financial barriers.[35]
- International Harmonization. Long-term progress requires convergence of rules and mutual recognition of certifications. Organizations such as the World Health Organization (WHO), the International Medical Device Regulators Forum (IMDRF), and the Organisation for Economic Co-operation and Development (OECD) are already offering international best-practice guides and model regulations.[36]

[32] International Organization for Standardization. ISO/IEC standards for biomedical sensors and clinical validation, e.g., ISO 80601-2-61. Geneva: ISO, 2017.
[33] HL7 International. Fast Healthcare Interoperability Resources (FHIR) Overview. Available at: https://www.hl7.org/fhir
[34] European Parliament and Council. General Data Protection Regulation (EU) 2016/679. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[35] Zinzuwadia S., Singh P. Digital inequality in wearable health technologies. Journal of Global Health, 2022. DOI: 10.7189/jogh.12.04067
[36] World Health Organization; International Medical Device Regulators Forum (IMDRF); Organisation for Economic Co-operation and Development (OECD). Guidelines and best practices for global medical device regulation, 2023

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


Technical and ethical issues are inseparably linked: the accuracy of data directly impacts fairness, while the protection of information underpins user trust[7]. Neither technology nor legislation alone is sufficient; a continuous dialogue among engineers, physicians, lawyers, and society is required.[37]

There is a positive trend: many countries are already implementing data-quality standards, interoperability protocols, and measures to broaden access. Yet the gap remains dynamic: new biosensors and AI-driven solutions demand flexible, proactive regulation. As the American Medical Association (AMA) emphasizes, "innovation moves quickly".[38]

## Conclusions

Wearable medical devices have the potential to transform healthcare by making continuous monitoring and early diagnosis accessible to far more people. But their real impact will depend on whether society can close the gap between rapid technological growth and slower legal and ethical adaptation. It is not enough to improve sensors or software alone. Governments need to update and align their regulations so that privacy, cybersecurity, and data accuracy are protected across borders. Public policy should focus on reducing inequality: lowering the cost of devices, supporting insurance coverage, and promoting digital literacy so that older adults, rural communities, and low-income groups are not left behind.

Manufacturers also carry a major responsibility. Security and ethical safeguards must be built in from the design stage, not added later as a patch. Open cooperation between developers, regulators, and healthcare providers can create a culture of accountability and faster, safer innovation. Progress will require an ongoing dialogue that includes engineers, doctors, lawyers, patient advocates, and ordinary users.

If these efforts continue, wearable technologies can grow under a reliable "safety net" of clear rules and shared standards. That combination of innovation, strong

[37] Canali S., Schiaffonati V., Aliverti A. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. PLOS Digital Health, 2022. DOI: 10.1371/journal.pdig.0000104

[38] Robeznieks A. Innovation in Digital Health Moves Quickly. American Medical Association, 2019. Available at: https://www.ama-assn.org

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


protections, and fair access is what will allow these devices to truly improve health outcomes and earn lasting public trust.

**References**

1. Bouderhem, R. (2023). Privacy and regulatory issues in wearable health technology. **Engineering Proceedings**, 58(1), 87. https://doi.org/10.3390/ecsa-10-16206
2. Canali, S., Schiaffonati, V., & Aliverti, A. (2022). Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. **PLOS Digital Health**, 1(3), e0000104. https://doi.org/10.1371/journal.pdig.0000104
3. European Parliament and Council. (2017). Regulation (EU) 2017/745 on medical devices (MDR). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2017/745/oj
4. European Parliament and Council. (2018). General Data Protection Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj
5. HL7 International. (2023). Fast Healthcare Interoperability Resources (FHIR): Overview and implementation guidance. https://www.hl7.org/fhir
6. IEEE Standards Association. (2024). IEEE P360—Wearable device interoperability standard (Draft). https://standards.ieee.org
7. International Medical Device Regulators Forum (IMDRF). (2023). Principles of international medical device regulatory convergence. https://www.imdrf.org
8. Robeznieks, A. (2019). Innovation in digital health moves quickly. **American Medical Association News**. https://www.ama-assn.org
9. U.S. Food and Drug Administration. (2018). De Novo classification request for Apple Watch ECG feature. https://www.fda.gov
10. U.S. Food and Drug Administration. (2023). Cybersecurity in medical devices: Quality system considerations and content of premarket submissions. https://www.fda.gov

*Modern American Journal of Social Sciences and Humanities*
**ISSN (E):** 3067-8153
Volume 01, Issue 06, September, 2025
**Website:** usajournals.org


11. Walter, A., et al. (2024). Patient-centered engineering of flexible wireless sensors for low-resource settings. **Nature Medicine**, 30(2), 245–258. https://doi.org/10.1038/s41591-024-03210-3
12. World Health Organization. (2021). Ethics and governance of artificial intelligence for health. https://www.who.int/publications/i/item/9789240029200
13. Zinzuwadia, S., & Singh, P. (2022). Digital inequality in wearable health technologies. **Journal of Global Health**, 12, 04067. https://doi.org/10.7189/jogh.12.04067