engineering proceedings

MDPI

Proceeding Paper

Privacy and Regulatory Issues in Wearable Health Technology †

Rabaï Bouderhem

College of Law, Prince Mohammad Bin Fahd University, P.O. Box 1664, Al Khobar 31952, Saudi Arabia; rbouderhem@pmu.edu.sa

† Presented at the 10th International Electronic Conference on Sensors and Applications (ECSA-10), 15–30 November 2023; Available online: https://ecsa-10.sciforum.net/.

Abstract: This paper is based on a research literature review for identifying and evaluating the technical, ethical and regulatory challenges to adequately regulate the use of wearable health technology. The objective is to analyze how researchers address the use of smart wearables in healthcare under the scope of data privacy. The main challenges faced by states in regulating e-health wearables were identified, especially the different methods to ensure the privacy of personal health information (PHI) and the legal voids and complexities to regulate wearable health technology at both national and international level. Finally, a few recommendations were made to regulate more efficiently wearable health technology at both national and international level. AI could be used as a regulatory tool to monitor the use of e-wearables in healthcare. Also, European Union (EU) law–upcoming EU Data Act and AI Act–can serve as models and guidance for the World Health Organization (WHO) which has a constitutional mandate to regulate the use of wearable health technology.

Keywords: data collection; health monitoring; privacy; regulations; smart wearables.

1. Introduction

Wearable [1] health technology is a global new trend which could disrupt healthcare by tracking health information in real-time. However, real-time health monitoring systems such as e-wearables also raise ethical and regulatory challenges regarding health data privacy. E-wearables collect, process, store and share considerable amount of data, including in the cloud from where third parties may be granted access to it [2]. The biggest challenge is data privacy [3] as health data is sensitive and confidential by nature [4]. It is important for all stakeholders–public and private actors–to find a consensus and an acceptable balance between regulation and innovation [5]. Technical, ethical and regulatory challenges such as data collection [6], data quality, security [7], interoperability between different operating systems (OS), health equity, and fairness [8] need to be addressed by states at both national and international level. Concrete national and international regulations should be developed such as the implementation of quality standards, conditions to access health data, interoperability, and representativity. Most importantly, compliance with key regulations such as the EU General Data Protection Regulation (GDPR) or the upcoming EU Data Act is a requirement. Self-regulation should also be encouraged as it will help to build public confidence in health wearable technology as important volumes of personal data are processed. Companies operating in this field are making efforts [9] and want to be seen as actors caring about personal health data and its processing, storing and sharing. Guidelines and voluntary codes of conduct developed by the private sector are concrete illustrations [10]. Despite the existence of such challenges, health wearables are an opportunity to improve healthcare systems as these devices could become a substantial addition to the everyday healthcare practice [11]. Indeed, health wearables could save lives as they act as computational systems allowing healthcare providers to adjust to patients' needs and situations; they can also be an important tool for people living in

Citation: Bouderhem, R. Privacy and Regulatory Issues in Wearable Health Technology. *Eng. Proc.* **2023**, *56*, x. https://doi.org/10.3390/xxxxx

Academic Editor(s): Name

Published: 15 November 2023

remote areas or far from hospitals or physicians [12]. As observed, there is today a global adoption of health wearables such as smartwatches or fitness trackers; this trend demonstrates that individuals have already embraced health wearable technology which could help monitoring people's health condition [13]. A balance between the use of health wearable technology and data privacy is a necessity from a regulatory and ethical perspective [14] as several challenges need to be solved. Different measures can be adopted to ensure privacy and security of health data; AI can also be used as a regulatory tool for audits and inspections in wearable health technology.

2. Challenges Posed by Wearable Health Technology

There are several challenges posed by wearable health technology ranging from technical [15] issues such as the development of powerful batteries to ethical and regulatory gaps at both national and international level. Data [16] accuracy is also a concern acknowledged by companies as physicians or lay people need precise data to be able to rely on it and monitor their health [17]. Data security [18] and privacy [19] are other crucial challenges to be addressed. Improper device wearing [20] could be another obstacle to health monitoring. From a scientific perspective, the use of consumer wearables [21] in health research could be a limitation as data may not be accurate (see Table 1 below).

Table 1. Challenges posed by wearable health technology.

Main Challenges Posed by Wearable Health Technology
1. Data privacy
2. Data collection and storage
3. Data quality and accuracy
4. Interoperability between different OS (Apple, Android, etc.)
5. Bias
6. Health equity
7. Access to technology in developing countries
8. Lack of regulations at both national and international level
9. Ability to control third parties' access to personal health data
10. Security

3. How Can We Ensure the Privacy and Security of Personal Health Data?

Different measures can be taken to ensure the privacy and security of personal health data [22]. Companies and health professional can help to secure patient privacy and data confidentiality (see Table 2 below).

Table 2. Measures to ensure privacy and security of personal health data.

Potential Measures and Safeguards for Effective Data Protection
1. Educate healthcare personnel
2. Conduct routine risk assessment
3. Secure data with a VPN
4. Restrict access to data
5. Implement role-based access
6. Two-factor authentication
7. Encryption
8. Security awareness training
9. AI to conduct regular inspections and audits to ensure compliance with regulations

It has been demonstrated [23] that most data breaches are attributable to human errors. Adequate training and education should be provided by healthcare institutions to

their personnel. Employees have to be well-aware of all risks associated with personal health data and security issues. Risk assessments on a regular basis are a requirement [24] as they could help to identify intrinsic limitations–such as data security breaches–of any healthcare institution and help to their resolution. Health personal data can also be protected and secured with a virtual private network (VPN) [25]. A VPN allows users to encrypt and mask their digital footprint. Healthcare institutions could protect themselves from data breaches and cyber-attacks such as ransomwares. Access to patients' health records has to be limited to certified personnel and restricted [26] for better data security and confidentiality. Healthcare institutions could implement improved authentication processes such as two-factor authentication. Based on the confidential and sensitive nature of health data, healthcare providers should implement role-based access control systems [27]; employees should only have access to a specific assigned system-level.

In the US, the Health Insurance Portability and Accountability Act (HIPAA) 1996 [28] regulates health data and ensures its security and confidentiality. As such, when physicians assign health wearables to their patients, all data collected is considered as protected health information (PHI). According to US federal regulations, all data collected, processed and shared must be protected and secured at all times [29]. Companies commercializing health wearables should consider first data privacy and security issues to be reliable alternatives to healthcare providers. This could be achieved through the adoption of international standards for e-wearables in sport for instance [30]. Health data privacy requires not only built-on security features, but also guarantees that the network is safe as well as third party applications available on the App Store or Google Store. Transparency [31] is a key aspect of data privacy as users should know who can access their data, whether it is a third party or the healthcare provider itself. Here, some gaps exist in the US legal framework applicable to health data and its handling. Indeed, HIPAA only targets specifically health data and not all wearables such as smartwatches which also collect health data. However, US authorities could provide a regulatory answer if such companies start dealing with health data and promote their products as health devices.

EU law offers today detailed rules and guidelines relating to privacy and the handling of personal data. The GDPR [32] is indeed a key regulation and a law model which offers a comprehensive legal framework with stringent obligations and duties for service providers and manufacturers [33]. Recently, the European Union Commission made a proposal [34] for a EU Data Act for adequate regulation of data specifically processed, stored or shared by electronic devices, including health wearables. In June 2023, the Council presidency and the European parliament came to a consensus and adopted the EU Data Act as a provisional agreement [35]. The objective of the EU Data Act is to harmonize rules relating to a fair access to data and its use by public and private actors. As its predecessor the GDPR, the EU Data Act will help wearable users to keep control over their health data more efficiently. It could also serve as a guideline or law model for the rest of the world and enshrine key international standards relating to health data privacy and security.

4. The Complexity to Regulate Wearable Health Technology at Both National and International Levels

The regulation [36] of wearable health technology at both national and international level is a complex issue but potential solutions exist (see Table 3 below).

Table 3. Solutions to adequately regulate wearable health technology at both national and international level.

Potential Solutions to Adequately Regulate Wearable Health Technology
1. Establishing clear guidelines and standards under WHO
2. Strengthening regulatory oversight
3. Promoting transparency and accountability
4. Encouraging industry self-regulation

5. Fostering international cooperation
6. Ethics in using personal health data

As stated, ethical and regulatory challenges need to be addressed by both states and international organizations such as the World Health Organization (WHO). There is a need for clear guidelines and standards [37] and how wearable health technology can help to promote healthcare systems worldwide. International guidelines and recommendations should be detailed as much as possible considering especially some important challenges such as accuracy, security, data privacy as well as ethics in the use of health wearables and data collected [38]. Ethical issues [39] with health wearable technology include users' data privacy, transparency and the necessity to ensure that users have given an informed consent to the processing of their personal data. Indeed, health wearables are small computers able to collect, process and store a considerable volume of personal data. Unauthorized access by third parties is an ethical issue and a violation of data privacy and informed consent [40]. Potential threats such as cybersecurity need to be tackled as well. Wearable health technology will play an important role in the near future as it facilitates health monitoring and can save lives. However, public authorities will need to create new regulatory bodies or give new powers and attribution to existing Watchdogs [41]. Throughout audits and inspections, regulatory bodies such as the FDA in the US and the Medicines and Healthcare products Regulatory Agency (MHRA) in the UK play a crucial role by monitoring all stakeholders and ensuring that they comply with their obligations in terms of privacy, efficiency, safety and quality. The promotion of transparency and accountability [42] is fundamental as companies know that they might face severe consequences such as financial sanctions, especially regarding their sharing [43] practices. They should also be held accountable for any breaches of data privacy or security. Self-regulation should be encouraged as codes of conduct can help to promote international standards such as data protection [44]. As mentioned, states and international organizations need to cooperate, harmonize their national regulations and promote the safe and ethical use of wearable health technology [45].

5. AI as a Regulatory Tool

Artificial Intelligence (AI) can play a key role in the regulation of wearable health technology [46]. AI tools already exist for a fast and reliable analysis of data [47] generated by wearables. AI can also identify deviations or anomalies in health measurements. This can help healthcare providers save lives but also allow them to make more accurate diagnosis or give better treatment. Regulatory authorities such as the FDA in the US and the MHRA in the UK can use AI to conduct regular inspections and audits to ensure compliance with established standards and regulations. At the international level, key players such as the European Union [48], the United Nations [49] (UN) and the WHO have also published proposals and guidance [50] on the ethical use of AI in healthcare. The objective of these regulations is to tackle the risks associated with the use of AI in healthcare. AI tools can help implement and regulate wearable health technology through data analysis, and facilitate compliance with established standards and regulations.

6. Conclusions

Blockchain technology can help build better healthcare systems. However, the novelty of this technology is source of ethical and regulatory challenges especially the necessity to comply with the right to privacy by protecting personal health data. Existing regulations such as the GDPR or upcoming ones such as the EU Data Act can provide reliable legal frameworks and established standards to be implemented by healthcare providers. States and international organizations such as the WHO need to cooperate and elaborate new guidelines and legally binding rules in this field. Also, AI promises to be a powerful tool with its ability to conduct automated audits and investigations.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Publicly available data.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Godfrey, A.; Hetherington, V.; Shum, H.; Bonato, P.; Lovell, N.H.; Stuart, S. From A to Z: Wearable technology explained. *Maturitas* **2018**, *113*, 40–47.
2. Escobar-Linero, E.; Muñoz-Saavedra, L.; Luna-Perejón, F.; Sevillano, J.L.; Domínguez-Morales, M. Wearable Health Devices for Diagnosis Support: Evolution and Future Tendencies. *Sensors* **2023**, *23*, 1678. https://doi.org/10.3390/s23031678.
3. Vidhi, K.; Singh, R.; Reddy, R.; Churi, P. Privacy issues in wearable technology: An intrinsic review. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC), Delhi, India, 20–22 February 2020.
4. da Silva, J.P. *Privacy Data Ethics of Wearable Digital Health Technology*; Center for Digital Health. 4 May 2023. Available online: https://digitalhealth.med.brown.edu/news/2023-05-04/ethics-wearables (accessed on).
5. Thierer, A.D. The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Richmond J. Law Technol.* **2015**, *21*.
6. Huarng, K.-H.; Yu, T.H.-K.; Lee, C.F. Adoption model of healthcare wearable devices. *Technol. Forecast. Soc. Chang.* **2022**, *174*, 121286.
7. Barua, A.; Al Alamin, M.A.; Hossain, M.S.; Hossain, E. Security and privacy threats for Bluetooth low energy in IoT and wearable devices: A comprehensive survey. *IEEE Open J. Commun. Soc.* **2022**, *3*, 251–281.
8. Canali, S.; Schiaffonati, V.; Aliverti, A. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. *PLoS Digit. Health* **2022**, *1*, e0000104. https://doi.org/10.1371/journal.pdig.0000104.
9. Chikwetu, L.; Miao, Y.; Woldetensae, M.K.; Bell, D.; Goldenholz, D.M.; Dunn, J. Does deidentification of data from wearable devices give us a false sense of security? A systematic review. *Lancet Digit. Health* **2023**, *5*, E239–E247.
10. Paul, M.; Maglaras, L.; Ferrag, M.A.; AlMomani, I. Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express* **2023**, *9*, 571–588.
11. Powell, D.; Godfrey, A. Considerations for integrating wearables into the everyday healthcare practice. *NPJ Digit. Med.* **2023**, *6*, 70. https://doi.org/10.1038/s41746-023-00820-z.
12. Canali, S.; Schiaffonati, V.; Aliverti, A. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. *PLoS Digit. Health* **2022**, *1*, e0000104. https://doi.org/10.1371/journal.pdig.0000104.
13. Loucks, J.; Stewart, D.; Bucaille, A.; Crossan, G. Deloitte Insights, Wearable Technology in Health Care: Getting Better All the Time, 1 December 2021. Available online: https://www2.deloitte.com/content/dam/insights/articles/GLOB164601_Wearable-healthcare/DI_Wearable-healthcare.pdf (accessed on).
14. Boumpa, E.; Tsoukas, V.; Gkogkidis, A.; Spathoulas, G.; Kakarountas, A. Security and Privacy Concerns for Healthcare Wearable Devices and Emerging Alternative Approaches. In *Wireless Mobile Communication and Healthcare. MobiHealth 2021*; Gao, X., Jamalipour, A., Guo, L., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Cham, Switzerland, 2022; Volume 440. https://doi.org/10.1007/978-3-031-06368-8_2.
15. Devine, J.K.; Schwartz, L.P.; Hursh, S.R. Technical, regulatory, economic, and trust issues preventing successful integration of sensors into the mainstream consumer wearables market. *Sensors* **2022**, *22*, 2731.
16. Azodo, I.; Williams, R.; Sheikh, A.; Cresswell, K. Opportunities and challenges surrounding the use of data from wearable sensor devices in health care: Qualitative interview study. *J. Med. Internet Res.* **2020**, *22*, e19542.
17. Smith, A.A.; Li, R.; Tse, Z.T.H. Reshaping healthcare with wearable biosensors. *Sci. Rep.* **2023**, *13*, 4998.
18. Dinh-Le, C.; Chuang, R.; Chokshi, S.; Mann, D. Wearable health technology and electronic health record integration: Scoping review and future directions. *JMIR Mhealth Uhealth* **2019**, *7*, e12861.
19. Banerjee, S.; Hemphill, T.; Longstreet, P. Wearable devices and healthcare: Data sharing and privacy. *Inf. Soc.* **2018**, *34*, 49–57.
20. Xue, Y. A review on intelligent wearables: Uses and risks. *Hum. Behav. Emerg. Technol.* **2019**, *1*, 287–294.
21. Sui, A.; Sui, W.; Liu, S.; Rhodes, R. Ethical considerations for the use of consumer wearables in health research. Digital Health **2023**, *9*, 20552076231153740.
22. Pirbhulal, S.; Samuel, O.W.; Wu, W.; Sangaiah, A.K.; Li, G. A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Gener. Comput. Syst.* **2019**, *95*, 382–391.
23. Hughes-Lartey, K.; Li, M.; Botchey, F.E.; Qin, Z. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon* **2021**, *7*, e06522.
24. Khan, F.; Kim, J.H.; Mathiassen, L.; Moore, R. Data breach management: An integrated risk model. *Inf. Manag.* **2021**, *58*, 103392.
25. Prabakaran, D.; Ramachandran, S. Multi-factor authentication for secured financial transactions in cloud environment. *CMC-Comput. Mater. Contin.* **2022**, *70*, 1781–1798.

26. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Secur. Appl.* **2023**, *1*, 100016.
27. Saha, S.; Chowdhury, C.; Neogy, S. A novel two phase data sensitivity based access control framework for healthcare data. *Multimed. Tools Appl.* **2023**, 1–26.
28. Edemekong, P.F.; Annamaraju, P.; Haydel, M.J. Health Insurance Portability and Accountability Act. [Updated 2022 Feb 3]. In *StatPearls*; StatPearls Publishing: Treasure Island, FL, USA, 2023. Available online: https://www.ncbi.nlm.nih.gov/books/NBK500019/ (accessed on).
29. Jayanthilladevi, A.; Sangeetha, K.; Balamurugan, E. Healthcare biometrics security and regulations: Biometrics data security and regulations governing phi and hipaa act for patient privacy. In Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 12–14 March 2020; pp. 244–247.
30. Ash, G.I.; Stults-Kolehmainen, M.; Busa, M.A.; Gaffey, A.E.; Angeloudis, K.; Muniz-Pardos, B.; Gregory, R.; Huggins, R.A.; Redeker, N.S.; Weinzimer, S.A.; et al. Establishing a global standard for wearable devices in sport and exercise medicine: Perspectives from academic and industry stakeholders. *Sports Med.* **2021**, *51*, 2237–2250.
31. Vidhi, K.; Singh, R.; Reddy, R.; Churi, P. Privacy issues in wearable technology: An intrinsic review. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC), Delhi, India, 20–22 February 2020.
32. EU General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
33. Mulder, T.; Tudorica, M. Privacy policies, cross-border health data and the GDPR. *Inf. Commun. Technol. Law* **2019**, *28*, 261–274. https://doi.org/10.1080/13600834.2019.1644068.
34. EU Commission, Press Release, 23 Feb. 2022, Brussels, Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 (accessed on).
35. Council of the EU, Press Release, 27 June 2023, Data Act: Council and Parliament Strike a Deal on Fair Access to and Use of Data. Available online: https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/data-act-council-and-parliament-strike-a-deal-on-fair-access-to-and-use-of-data/#:~:text=The%20data%20act%20will%20give,objects%2C%20machines%2C%20and%20devices (accessed on).
36. Iqbal, J.D.; Biller-Andorno, N. The regulatory gap in digital health and alternative pathways to bridge it. *Health Policy Technol.* **2022**, *11*, 100663.
37. Espinoza, J.; Xu, N.Y.; Nguyen, K.T.; Klonoff, D.C. The need for data standards and implementation policies to integrate CGM data into the electronic health record. *J. Diabetes Sci. Technol.* **2023**, *17*, 495–502.
38. Taka, A.M. A deep dive into dynamic data flows, wearable devices, and the concept of health data. *Int. Data Priv. Law* **2023**, *13*, 124–140.
39. Leese, J.; Zhu, S.; Townsend, A.F.; Backman, C.L.; Nimmon, L.; Li, L.C. Ethical issues experienced by persons with rheumatoid arthritis in a wearable-enabled physical activity intervention study. *Health Expect.* **2022**, *25*, 1418–1431.
40. Segura Anaya, L.H.; Alsadoon, A.; Costadopoulos, N.; Prasad, P.W.C. Ethical Implications of User Perceptions of Wearable Devices. *Sci. Eng. Ethics* **2018**, *24*, 1–28. https://doi.org/10.1007/s11948-017-9872-8.
41. Korjian, S.; Gibson, C. M. Digital technologies and the democratization of clinical research: Social media, wearables, and artificial intelligence. *Contemp. Clin. Trials* **2022**, *117*, 106767.
42. Tahri Sqalli, M.; Aslonov, B.; Gafurov, M.; Nurmatov, S. Humanizing AI in medical training: Ethical framework for responsible design. *Front. Artif. Intell.* **2023**, *6*, 1189914.
43. Banerjee, S.; Hemphill, T.; Longstreet, P. Wearable devices and healthcare: Data sharing and privacy. *Inf. Soc.* **2018**, *34*, 49–57.
44. Winter, J.S.; Davidson, E. Harmonizing regulatory regimes for the governance of patient-generated health data. *Telecommunications Policy* **2022**, *46*, 102285.
45. Colloud, S.; Metcalfe, T.; Askin, S.; Belachew, S.; Ammann, J.; Bos, E.; Kilchenmann, T.; Strijbos, P.; Eggenspieler, D.; Servais, L.; et al. Evolving regulatory perspectives on digital health technologies for medicinal product development. *NPJ Digit. Med.* **2023**, *6*, 56.
46. Venkatesh, K.P.; Raza, M.M.; Kvedar, J.C. Health digital twins as tools for precision medicine: Considerations for computation, implementation, and regulation. *NPJ Digit. Med.* **2022**, *5*, 150.
47. Padoan, A.; Plebani, M. Flowing through laboratory clinical data: The role of artificial intelligence and big data. *Clin. Chem. Lab. Med. (CCLM)* **2022**, *60*, 1875–1880.
48. EU Commission. Brussels, 21.4.2021, COM(2021) 206 Final, 2021/0106(COD), Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (accessed on).

49. United Nations. UN Decade of Healthy Ageing. United Nations. Available online: https://www.who.int/initiatives/decade-of-healthy-ageing (accessed on).
50. *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*; World Health Organization: Geneva, Switzerland, 2021. Available online: https://www.who.int/publications/i/item/9789240029200 (accessed on).