Understanding Privacy Concerns in the Rise of Wearable Healthcare Devices

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Jaimin Thakkar

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent Wayland, Department of Engineering and Society

INTRODUCTION

Wearable health devices, such as smartwatches and fitness trackers, have become common tools for tracking physical activity, heart rate, sleep patterns, and other health measurements. These types of devices are also being introduced into clinical settings, where they assist in remote patient monitoring and management. While these devices provide better access to health information, they also raise concerns about privacy, consent, and trust in how patient data is collected, stored, and shared. In healthcare settings, wearable devices specifically refer to clinical-grade technologies like continuous glucose monitors, wearable electrocardiograms (ECGs), remote patient monitoring patches, and pulse oximeters rather than consumer-grade fitness trackers.

The main question this research paper addresses is: How can wearable technologies in healthcare, powered by machine learning, improve patient outcomes while addressing ethical challenges like privacy, trust, and informed consent?

As these devices become more involved in healthcare decisions, patients, healthcare providers, and developers face challenges in securing data and ensuring ethical use. Understanding these challenges is important to ensure responsible development and safe use of wearable health technology in medical environments.

Wearable health devices function as portable medical assistants. It collects real-time health data from users and transmitting it to cloud-based platforms or healthcare providers. They track key health factors such as heart rate, blood pressure, blood oxygen levels, and activity levels. For example, devices like continuous glucose monitors measure blood sugar levels continuously for

diabetic patients, and wearable ECG monitors detect abnormal heart rhythms which allows for early diagnosis. In clinical settings, hospitals use wearable devices to monitor patients continuously without requiring them to stay under direct supervision. Patients with heart disease may wear ECG monitors, and post-surgical patients may use motion trackers to assess recovery progress. These devices assist in predictive health analysis. Where machine learning models analyze collected data to detect early signs of health deterioration. However, the effectiveness of these devices depends on accurate data collection, proper device function, and strong security measures.

The challenges with wearable health devices start with their dependence on continuous data transmission. They must send sensitive patient data through wireless networks, making them vulnerable to risks of unauthorized access. Unauthorized access or data breaches could expose private health information to third parties, such as insurance companies or advertisers. Furthermore, device accuracy is another concern where incorrect readings can lead to misdiagnosis or unnecessary medical intervention. In hospitals, inaccurate oxygen level detection in COVID-19 patients using pulse oximeters was a notable case where wearable technology failed to perform equally across different populations, and it affected trust in these devices.

Another major factor in wearable health devices is regulatory oversight. Governments and health agencies such as the FDA in the U.S. and the European Medicines Agency (EMA) regulate wearable health technology. But these regulations often lag the pace of technological advancement. As new health-tracking features are added, companies must balance innovation and compliance with data protection laws. The Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in Europe outline

how medical data should be protected, but wearable devices operate in grey areas where personal and medical data overlap. This lack of clarity in laws creates challenges for both patients and device manufacturers.

Background & Context

Sociotechnical Situation

Wearable health devices in clinical settings are designed to extend healthcare beyond the traditional hospital environment. These devices are typically clinical-grade sensors that monitor vital signs like heart rate variability, blood glucose levels, respiratory patterns, and body temperature. Examples include wearable ECG monitors for cardiac patients, continuous glucose monitors for diabetic management, wearable blood pressure cuffs, and smart patches that track multiple health metrics simultaneously. They are lightweight, wireless, and capable of transmitting real-time health data to healthcare providers, who can then intervene promptly when abnormal readings are detected.

The integration of wearable technology into hospitals and clinics allows doctors to monitor patients remotely and reduce the need for prolonged hospital stays. It also provides proactive healthcare management. For instance, patients recovering from surgery might wear a wireless ECG patch that sends continuous data to their doctor, who can monitor for potential complications without requiring the patient to stay admitted. Another example includes continuous oxygen saturation monitors used in managing COVID-19 patients remotely to detect early signs.

However, this technological advancement has introduced new complications. The infrastructure supporting wearable devices such as cloud storage systems and wireless networks has security vulnerabilities. Health data is transmitted through Wi-Fi, Bluetooth, or cellular connections which exposes it to interception or breaches. If these systems are not properly secured, sensitive health information could be accessed by unauthorized parties, and it risks patient privacy and violating legal protections.

Moreover, many wearable devices operate with machine learning algorithms that detect health anomalies or predict risk factors. These algorithms rely heavily on historical datasets, but these datasets may contain biases based on race, age, gender, or socio-economic status. For example, early versions of wearable heart rate monitors were found to be less accurate for individuals with darker skin tones, because the sensors reflected differently off darker skin pigments. This raises ethical concerns about fairness and inclusiveness in wearable health technologies.

Another sociotechnical challenge involves informed consent. Traditionally, medical interventions are accompanied by clear consent procedures, but wearable devices blur these boundaries. When a patient agrees to wear a glucose monitor or a cardiac patch, they might not fully understand how their data is collected, how frequently it is transmitted, or who ultimately has access to it beyond their immediate medical team. This lack of transparency can lead to an issue of patient trust, particularly if data is shared with insurance companies, pharmaceutical firms, or tech companies without explicit permission.

Finally, the regulation of wearable health devices has not kept pace with innovation. Regulatory bodies like the FDA have frameworks for medical devices, but the unique nature of continuous, passive data collection by wearables challenges traditional regulatory models. Furthermore,

devices classified as "wellness tools" rather than "medical devices" often bypass rigorous approval processes altogether, even though they may be used for serious clinical purposes. This regulatory gray area complicates accountability when errors occur or when breaches happen.

In short, wearable health devices are reshaping the boundaries between patients, healthcare providers, and technology developers. They offer incredible opportunities to improve patient outcomes but simultaneously create new ethical, legal, and technical challenges that require careful consideration from all stakeholders involved in the healthcare system.

Literature Review

Wearable healthcare devices present new opportunities and challenges in clinical settings. Trust and data security are two of the most important concerns for users. Studies show that patients are more likely to use wearable devices if they trust that their personal health information is properly secured and handled (He et al., 2019). However, gaps in regulation, especially for cloud-based data storage, create risks that current privacy laws like HIPAA do not fully cover (BMC Medical Ethics, 2021).

Bias in wearable device algorithms is another major issue. Research highlights that machine learning models built using non-diverse datasets can create inaccurate predictions, especially for minority populations (Jiang et al., 2017). For example, wearable devices that measure heart rate and blood oxygen levels have sometimes been less accurate for individuals with darker skin tones, leading to potential health disparities (Canali, Schiaffonati, & Aliverti, 2022).

The ethical challenges of wearable devices also include concerns about continuous data collection. Many users are not fully aware of the extent of personal information being gathered

by these devices, raising questions about informed consent (Vayena et al., 2018). Unlike traditional clinical procedures where patients actively agree to tests, wearable devices often collect data passively, sometimes without users even realizing it (American Journal of Health-System Pharmacy, 2024).

Corporate responsibility plays an important role as well. Manufacturers of wearable devices often focus more on profit than transparency and making users rely on blind trust that their health data is protected (CDC, 2024). Additionally, studies note that current policies are not fully designed to address real-time, continuous health data generated by wearable devices, creating further gaps in user protection (Williamson et al., 2024).

Overall, the existing research highlights that while wearable healthcare devices offer a lot of benefits like remote monitoring and early detection of health issues, they also bring major risks. Privacy breaches, biased algorithms, and lack of user understanding about consent could limit the ethical use of these technologies. The literature shows the need for stronger regulations, transparent device designs, and better education for users to make sure that wearable healthcare devices truly improve patient care without compromising trust and fairness.

Theoretical Framework: SCOT Approach

The Social Construction of Technology (SCOT) framework helps explain how wearable healthcare devices are shaped by the people and groups that use and regulate them. SCOT argues that technology does not develop on its own based only on technical improvements. Instead, it evolves depending on how different social groups, like patients, doctors, hospitals, regulators,

and manufacturers, view and use it. In the case of wearable health devices, patients may see these devices as a way to get more control over their health. Doctors and hospitals may view them as tools to improve patient monitoring and reduce hospital visits. Regulators might focus on safety, privacy, and ethical use. Manufacturers often look at ways to make these devices more appealing to consumers.

Interpretive flexibility is an important part of SCOT. It means that different groups can see and use the same technology in different ways. For example, a wearable device that tracks heart rate could be seen by patients as a preventive health tool, while insurers might see it as a way to collect more data about customer health risks. Over time, negotiations and power dynamics among these groups lead to certain features or designs becoming dominant. For instance, the push for stronger encryption in wearable devices did not arise only because it was technically possible. It happened because patients, privacy advocates, and healthcare institutions demanded better protection of health information.

In wearable healthcare technology, SCOT shows us that concerns over privacy, bias, and consent are not side issues as they are built into how the technology itself develops. As more people push for transparency, fairer machine learning algorithms, and better regulation, wearable health devices will likely continue to change. Using SCOT as a guide helps us understand that these devices are not finished products, and they are part of an ongoing negotiation between technology and society.

Methods

The research for this paper is based on a qualitative analysis of existing literature, case studies, and government or organizational reports related to wearable health devices, privacy concerns, consent challenges, and trust in healthcare settings. The goal was to collect information that would help answer the question: how concerns about privacy, consent, and trust shape the design and use of wearable health devices in hospitals and clinics.

Sources were chosen carefully to ensure a wide view of the situation. Peer-reviewed academic journal articles were selected through searches on Google Scholar, PubMed, and PLOS Digital Health. Search terms included "wearable health devices," "privacy in wearable technology," "machine learning in healthcare," and "ethical challenges of health devices." Literature from 2018 to 2024 was prioritized to focus on recent developments. Two specific case studies, one during the COVID-19 pandemic and another involving Mayo Clinic's wearable technology projects were selected for detailed analysis because they clearly showed how society and technology shaped each other in healthcare environments.

Evidence collected included examples of real-world failures, privacy breaches, successful deployments of wearable technology, and surveys about patient attitudes toward wearable devices. For all sources, only those coming from reputable journals, health organizations, or university presses were used to ensure the information was credible and reliable. The focus was on highlighting concerns from patients, clinicians, and developers about privacy, consent, and trust in healthcare data collection practices.

The analysis involved identifying patterns and recurring themes related to privacy challenges, informed consent procedures, bias in device performance, and regulatory gaps. These patterns were then connected back to the idea of mutual shaping and the SCOT framework to show how social concerns actively influence the technical development and deployment of wearable health technologies.

Case Study 1: Remote Monitoring of COVID-19 Patients Using Wearable Technology

The COVID-19 pandemic presented new challenges for healthcare systems, particularly in monitoring patients remotely to reduce hospital overcrowding and minimize virus transmission. A study conducted by researchers at Wellcome Open Research explored how wearable technology could support the remote management of COVID-19 patients. This case study highlights the potential and challenges of implementing wearable health devices in clinical crisis settings.

The study focused on using wearable sensors that continuously monitored patients' vital signs, such as oxygen saturation, heart rate, respiratory rate, and body temperature. Patients who tested positive for COVID-19 but were not critical enough for immediate hospitalization were given wearable devices to track their health status from home. The information collected was transmitted to a centralized monitoring system where healthcare professionals could review the data in real time. By detecting early signs of deterioration, clinicians could intervene quickly, often before the patient's condition became life-threatening (Chau et al., 2023).

One major advantage of the wearable monitoring system was its ability to alert medical staff when a patient's oxygen saturation dropped below safe thresholds, a key indicator of worsening

COVID-19 symptoms. Early detection of "silent hypoxia," where patients do not feel breathless despite dangerously low oxygen levels, proved critical for timely medical intervention (Chau et al., 2023). Without the help of wearable devices, many patients could have gone undetected until they reached a severe stage which required intensive care.

However, the study also showed several limitations. Some patients struggled with the proper use of wearable devices at home, and it led to data inaccuracies. Connectivity issues and user errors sometimes resulted in missing data points which required manual follow-up by healthcare teams. In addition, concerns about patient privacy emerged, particularly regarding the continuous collection and transmission of sensitive health data outside a secured clinical environment. While patients generally accepted the monitoring because of the pandemic's urgency, there were still questions about how the data might be used beyond immediate care needs (Chau et al., 2023).

Another challenge was ensuring equity of access. The study found that not all patients had the technological literacy or reliable internet access needed to effectively use the wearable monitoring system (Chau et al., 2023). This digital divide risked leaving behind vulnerable populations, such as the elderly and those from lower socioeconomic backgrounds. To address this, the researchers suggested incorporating user-friendly device designs and providing clear educational support for patients when wearable technology is deployed for remote monitoring.

Overall, the COVID-19 remote monitoring initiative showed how wearable health devices could become essential tools during health emergencies. It demonstrated how technology, when properly integrated into healthcare systems, can extend care beyond hospital walls, improve early detection of critical conditions, and potentially save lives. At the same time, it emphasized the

importance of addressing challenges around usability, data privacy, and equitable access to ensure that wearable technology serves all populations fairly and effectively.

Case Study 2: Mayo Clinic's Use of AI in Clinical Decision-Making

The Mayo Clinic has emerged as a leader in adopting artificial intelligence (AI) to support clinical care, especially during the COVID-19 pandemic. This case study explores how Mayo Clinic integrated AI into diagnostic imaging, remote care, and decision-making while also managing ethical concerns related to transparency and data privacy. Their experience offers a valuable example of how AI can be used to improve healthcare outcomes while maintaining trust.

One major area where Mayo Clinic applied AI was in diagnostic imaging. The institution developed machine learning models to help radiologists interpret CT scans and MRIs more efficiently, especially during the surge of COVID-19 cases (Farrugia & Plutowski, 2020).

These tools helped identify subtle signs of disease that could be missed during manual reviews. It improved both diagnostic accuracy and turnaround time. Researchers in China had similarly used AI to reveal distinctions in CT scans for COVID-19, and Mayo's use of such tools placed them at the forefront of imaging innovation.

Mayo Clinic also expanded remote care through the use of AI-powered virtual health systems. The organization accelerated efforts to integrate in-person and remote care by launching advanced home care programs (Farrugia & Plutowski, 2020). These relied on physician-led, 24/7 remote monitoring supported by AI systems. The tools allowed clinicians to track patient data in real time, helping them make faster decisions while keeping patients safely at home. By

combining technology with human oversight, Mayo ensured that AI complemented rather than replaced clinical judgment.

To ensure trust in these AI tools, Mayo focused on transparency. The clinic prioritized the use of explainable AI systems that allowed physicians to understand how decisions were made (Farrugia & Plutowski, 2020). This approach helped clinicians interpret model outputs and decide when to trust or challenge the recommendations. Maintaining physician authority and reinforcing that AI was only a support tool helped uphold clinical ethics and patient safety.

Data security and patient consent were additional areas of focus. As AI systems require access to large datasets, Mayo implemented strict safeguards to ensure that sensitive health information was protected. The article describes the institution's investment in secure digital systems and virtual infrastructure that supported responsible data use (Farrugia & Plutowski, 2020). Patients were informed when their anonymized data were used to improve AI models, helping preserve both ethical standards and public confidence.

In summary, Mayo Clinic's strategic use of AI during the pandemic highlights how healthcare institutions can embrace innovation while maintaining ethical boundaries. By focusing on transparency, clinical oversight, remote care expansion, and secure data use, Mayo offered a model that others can follow when introducing AI into healthcare.

Discussion/Analysis

The growing use of wearable health devices in clinical settings clearly shows the mutual shaping of technology and society. Society's increasing demand for more accessible and real-time healthcare has driven the rapid development of wearable health technologies. At the same time,

the design, deployment, and regulation of these devices are being influenced by public concerns over privacy, trust, and consent. The COVID-19 case showed how urgent healthcare needs can push society to accept new technologies quickly, even if the privacy implications are not fully understood. On the other hand, the Mayo Clinic case highlights that thoughtful planning and attention to ethical concerns can make wearable health technology a trusted part of medical care.

One important point from both case studies is that trust is not automatic. Healthcare institutions must work deliberately to build it by being transparent about data use and ensuring strong protections. Patients expect not only technical reliability from these devices but also ethical responsibility from the people who manage their data. The case of COVID-19 showed that rushing new technologies without strong consent policies can damage public trust, while Mayo Clinic's careful consent processes showed a way forward.

Another key issue is bias. As wearable devices become part of healthcare decision-making, ensuring that devices work equally well across diverse populations becomes crucial. Machine learning models trained on biased datasets could worsen existing health inequalities. Companies and healthcare providers must invest in better testing and training practices to prevent these issues.

Finally, the cases suggest that technology adoption in healthcare cannot be separated from the social environment. Policies, social trust, public health needs, and technology design all interact continuously. The SCOT framework helps explain this by showing that wearable health technology is shaped by groups like patients, doctors, developers, and regulators, and that the final form of the technology is never fixed. It keeps evolving in response to social pressures and needs.

Conclusion

Wearable healthcare devices have transformed how patients and providers interact with health information. These devices, from hospital-grade monitors to advanced trackers, allow for real-time monitoring, early detection of health issues, and greater patient independence. However, along with these benefits come serious concerns about data privacy, consent, trust, and bias. Throughout this paper, it explored how different groups shape the technology's design and use, as explained by the SCOT framework. It also talked about real-world case studies that show how wearable devices perform under real conditions which highlighted both successes and challenges.

The research shows that while wearable health devices offer clear clinical value, their success depends on addressing the social and ethical challenges around them. Patients' trust relies on how well their data is protected. Healthcare providers depend on device accuracy to make life-impacting decisions. Manufacturers need to prioritize transparency and fairness, especially when designing AI models that process health data. Regulators must keep pace with rapid technological advances to ensure patient rights are protected. These layers of influence confirm that wearable health technologies are part of a larger sociotechnical system shaped by human concerns, not just technical innovation.

Moving forward, better regulations, improved technology design, and more informed patients are key to the responsible use of wearables in healthcare. Developers must create devices that are inclusive, accurate, and transparent. Healthcare systems must educate both patients and providers on the benefits and risks of using wearables. Policymakers need to close regulatory gaps to

ensure continuous protection of patient data. Finally, researchers must continue studying the evolving relationship between society and health technology to guide future innovation.

Wearable healthcare technology has incredible potential to improve outcomes, reduce healthcare costs, and empower patients. But realizing that potential will depend on maintaining a careful balance between innovation and ethical responsibility. The way society and technology shape each other will decide whether wearable healthcare devices fulfill their promise or fall short.

LITERATURE REVIEW

American Journal of Health-System Pharmacy. (2024). Ethical implications of wearable digital health technology: Balancing innovation and patient autonomy. *American Journal of Health-System Pharmacy.* https://ajhcs.org/article/ethical-implications-of-wearable-digital-health-technology-balancing-innovation-and-patient-autonomy

BMC Medical Ethics. (2021). Privacy and artificial intelligence: Challenges for protecting health information. *BMC Medical Ethics, 22*(1). https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-021-00687-3

Canali, S., Schiaffonati, V., & Aliverti, A. (2022). Challenges and recommendations for wearable devices in digital health. *PLOS Digital Health.* https://journals.plos.org/digitalhealth/article?id=10.1371%2Fjournal.pdig.0000104

Centers for Disease Control and Prevention. (2024). Health equity and ethical considerations in using artificial intelligence in public health and medicine. *Preventing Chronic Disease, 21*(4). https://www.cdc.gov/pcd/issues/2024/24_0245.htm

Chau, N. V. V., Trung, T. N., et al. (2023). Wearable devices for remote monitoring of hospitalized patients with COVID-19 in Vietnam [version 2; peer review: 3 approved, 1 approved with reservations]. *Wellcome Open Research, 7*, 257. https://doi.org/10.12688/wellcomeopenres.18026.2

Farrugia, G., & Plutowski, R. W. (2020). Innovation Lessons From the COVID-19 Pandemic. Mayo Clinic Proceedings, 95(8), 1574–1577. https://doi.org/10.1016/j.mayocp.2020.05.024

He, J., Baxter, S. L., Xu, J., Zhou, X., Zhang, K., & Li, S. (2019). The practical implementation of artificial intelligence technologies in medicine. *Nature Medicine, 25*(1), 30–36. https://doi.org/10.1038/s41591-018-0307-0

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., & Wang, Y. (2017). Artificial intelligence in healthcare: Past, present, and future. *Stroke and Vascular Neurology, 2*(4), 230–243. https://svn.bmj.com/content/2/4/230

Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. *PLOS Medicine, 15*(11), e1002689. https://doi.org/10.1371/journal.pmed.1002689

Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences, 14*(2), 675. https://doi.org/10.3390/app14020675