International Journal of Safety and Security Engineering
Vol. 16, No. 2, February, 2026, pp. 307-326
Journal homepage: http://iieta.org/journals/ijsse

# Wearable Health IoT Devices: A Vision on Compliance, Security and Feature Directions

Sheetal V A*, Jyothi S Nayak

Department of CSE, B.M.S College of Engineering, Bengaluru 560019, India

Corresponding Author Email: gdsheetal26@gmail.com

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.160206

**Received:** 15 November 2025
**Revised:** 13 February 2026
**Accepted:** 20 February 2026
**Available online:** 28 February 2026

***Keywords:***
*legal regulations, technical and ethical compliance, health insurance port-ability and accountability act, general data protection regulation, California's consumer privacy act, food and drug administration, medical devices regulation, wearable IoT*

**ABSTRACT**

Wearable fitness trackers, heart rate monitors, and sleep wearables are transforming personal healthcare by gathering data all the time and giving people personalized insights. Even with these improvements, widespread use presents problems with the law, technology, and ethics. This article lists problems and solutions for wearable health IoT devices that track sleep, fitness, and heart rate. The review looks at data privacy standards from around the world and healthcare-specific rules to uncover areas where they don't match up or are not being followed. A classification framework divides compliance needs into three groups: legal, technological, and ethical. These groups include data protection, medical device laws, security methods, privacy-by-design, informed consent, data ownership, and algorithmic fairness. The key findings are that the international legal framework remains non-harmonized, privacy-saving technology is not being implemented effectively on devices of limited resources, and ethical concerns of transparency and bias still exist. The article talks of encryption architectures, safe data governance model, and ethical design requirements as a way of dealing with these problems. The paper highlights the significance of clear regulatory standards, automated compliance and justice and fair play in the design of wearable IoT systems and also pinpoints open research directions. This study supports the development of adherent, safe, and dependable health wearable technologies under a holistic perspective.

## 1. INTRODUCTION

The wearable Internet of Things (IoT) technologies have been very popular over the past few years. All the time, millions of people wear smartwatches, fitness trackers, and sleep monitors to monitor their health. Such devices allow gathering physiological and behavioral information in real time, which assists in personalized healthcare, early diagnosis, and preventive therapy. Wearable health IoT systems are increasingly becoming part of our daily lives and, therefore, are gathering numerous personal data points, which brings up some serious concerns about data protection, system security, and rule compliance. Trends in personalized medicine and remote monitoring have precipitated the global attention to wearable IoT in healthcare, which is further increased by the COVID-19 pandemic that highlighted the importance of monitoring health-related data beyond the clinical environment [1, 2]. An example is that, as of 2022, more than one-third of adults in the U.S. were wearing a health-related wearable, which was 14% higher than in the past years. The advantages of these wearables include early warning of abnormalities (e.g., irregular heartbeats), better interaction with patients, and big data in health research [3, 4].

The wearable IoT devices lie at the nexus of technology, healthcare, and personal data that pose complex problems in legal, technical, and ethical spaces [5]. It is noteworthy that the issue of privacy and data protection has been recognized as a primary issue in wearable health technology. Wearables constantly monitor sensitive personal health data, heartbeat rates, sleep patterns, and physical activity data, and it is frequently sent to cloud applications or third-party software. The real-time gathering and sharing of sensitive data brings grave requirements in the data protection law and heightens the privacy issues of the users. The data is highly personal (and can reveal medical conditions), and its misuse or unauthorized use will be catastrophic. The creators and producers of wearables have had a big challenge in ensuring that they comply with the law that is meant to protect such data.

In terms of the legal aspect, wearable health devices are currently in a mess of legal systems. The General Data Protection Regulation (GDPR) that is currently operational in the European Union is quite strict in the processing of personal data and requires some legal justification (including user consent), minimization, and proper security of any information concerning health [6, 7]. In the US, health data privacy is, in turn, governed by industry-specific legislation, such as the Health Insurance Portability and Accountability Act (HIPAA). Wellness wearables and HIPAA Consumer wellness wearables might not necessarily be subject to HIPAA where the information is not processed by a covered medical entity, which can create grey areas of regulation [8, 9]. This distinction explains why it is hard to find a balance with the transfer of equipment and personal information across jurisdictions and legal definitions. These regulatory frameworks will be discussed in the following sections.

Also significant are the technical compliance issues. The

size, power, and compute capabilities of wearable IoT devices can make it challenging to enforce strong security and privacy controls. A number of wearables have been found to transmit data in a nonsecure manner or gather additional data than required [6, 10]. Security assessment shows that the communication protocols (e.g., Bluetooth Low Energy) have weaknesses which may allow personal information to be compromised unless well addressed. Protecting privacy-by-design - incorporating data protection capabilities such as encryption and anonymization - are often considered a trade-off to the performance and battery life of the devices [7, 11]. We examine the role of these technical problems in deterring compliance, and solutions to the problems under discussion.

Other than the law and technology, ethical compliance and the trust of the end-users will be of utmost importance to popularizing health wearables. The users should be assured that their intimate health data is being dealt with ethical and transparent methods. Such challenges as informed consent, ownership of data, and algorithmic fairness become prominent [12, 13]. For example, if a wearable's analytic algorithm is biased or less accurate for certain populations, it could exacerbate health disparities – an ethical concern receiving increased attention [5, 13]. Similarly, the pervasive tracking by wearables raises questions about user autonomy and the potential for surveillance or misuse of data by third parties (employers, insurers, etc.) [8, 14]. Surveys indicate that while many consumers are willing to share wearable data for health benefits, they remain concerned about who else accesses their data and for what purposes [9, 14].

This paper will provide a thorough analysis of compliance considerations and issues of wearable IoT devices in medical and wellness monitoring. We take a holistic approach that encompasses legal regulations that regulate wearable data (Section 2), the difficulties in complying with them (Section 3), and how we will select literature and categorize the issues of compliance (Section 4). Next, we move on to domain-specific discourse: the compliance issues of wearable IoT (Section 5), and the frameworks and solutions that are already available to guarantee compliance (Section 6). Lastly, we point out open research problems and future research (Section 7) that need to be resolved to balance innovation in wearable health tech and high compliance. Encryption and Authentication to Compliance in Wearable IoT Health Devices is addressed (section 8), and a number of Case Studies of Compliance Failures in Wearable/Medical IoT Devices (section 9). This work, by connecting the perspectives of law, technology, and ethics, will help stakeholders, including device manufacturers, healthcare providers, policymakers, and researchers, develop wearable IoT devices that are innovative, effective, and legally secure, and respectful of user rights.

This research aims to critically examine compliance concerns and remedies in wearable health IoT systems, specifically, the fitness, heart rate, and sleep monitoring devices. The research addresses the following key questions: (i) What are the legal, technical, and moral requirements that wearable health IoT systems have to fulfill? (ii) What are the largest issues that should be addressed to achieve compliance across these areas? (iii) What are the solutions and frameworks proposed to address such problems?

In this paper, a systematic and extensive view of compliance has been provided by providing a three-dimensional classification framework that encompasses legal, technical, and ethical, unlike previous surveys that primarily focus on security or generic IoT healthcare applications. The paper offers an in-depth understanding of compliance with wearable health IoT through the combination of regulatory analysis, technical mechanisms, and ethical concerns. It also identifies critical gaps and proposes areas to conduct additional research.

## 2. COMPLIANCE AND LEGAL REGULATIONS

Wearable health devices exist in a complicated legal environment that includes data protection law, health-related regulations, consumer protection and others. Here, we provide an overview of the most important legal and regulatory frameworks in the context of wearable IoT compliance, including their requirements and the impact on the device monitoring fitness, heart rate, sleep, and other health indicators.

Data Protection and Privacy Laws: The most significant legal implications of wearables revolve around data privacy laws. Since wearables are known to gather personal information (which can be sensitive health data), general data protection regulations such as the GDPR implemented by the EU and other countries around the globe are relevant. The GDPR (which took effect in 2018) places significant expectations on how personal data is handled, and it has an extensive territorial reach, which covers any wearable company that processes data of EU residents. In GDPR, health-related data is considered a special category of sensitive data with a higher level of protection [15]. Compliance involves user-informed consent (or other legitimate legal basis) to process data, only collect necessary (data minimization) data, and have proper technical and organizational controls in place. Practically, a lot of wearable items have failed to conform to these principles. Research has discovered that wearables can gather too much information that is inconsistent with the principle of minimization of GDPR, and the privacy policies might not effectively alert users, which is a flaw in the consent principle. As an illustration, one of the fitness tracker apps had been analyzed, and it was observed that certain applications were requesting permission to access phone sensors (e.g., microphone, contacts) with no evident justification, so they violated GDPR standards. Transparency and purpose limitation are legal requirements, but compliance audits show that wearable privacy announcements are sometimes unclear or excessively generative, giving the user no idea how they will use their information.

The US has no federal data protection law that is comparable to GDPR. Rather, a patchwork of laws is used. HIPAA governs medical data privacy and security, but is largely limited to "covered entities" (healthcare providers, insurers, and their business associates). Data generated by consumer-owned wearables typically falls outside of HIPAA's coverage if it is not shared with a covered healthcare provider. This means companies like fitness tracker manufacturers are generally not bound by HIPAA's Privacy Rule, creating a regulatory gap for health data collected directly by consumers [8, 9]. As a result, sensitive physiologic data from a smartwatch might not receive the same legal protection as data in an electronic medical record. Some states have begun addressing this gap – for instance, California's Consumer Privacy Act (CCPA) gives consumers rights over personal data, and would include fitness data held by a company – but state laws vary in scope and enforcement. Scholars have highlighted that the U.S. reliance on notice-and-consent

frameworks (via privacy policies and terms of service) places the burden on consumers to manage their privacy, which is often ineffective [8]. By simply clicking the I agree button and not reading long policies, users are effectively waiving privacy without actually having to read the policies in practice [8, 16]. This self-management model has been criticized as inadequate compared to the wearables, where information streams are continuous and intricate.

Other jurisdictions have implemented or revised laws that regulate data protection that are relevant to wearable data. As an example, the Personal Data Protection Bill (since the Data Protection Act, 2023) of India [17] and similar regulations in countries like Australia, Brazil, and Japan incorporate provisions for handling sensitive personal data, which would include health metrics from wearables. These regulations are more or less reflected in the principles of consent, purpose restriction, and security. The issue with wearable manufacturers is that they not only need to meet a number of different legal regimes. An item that is sold worldwide might be required to comply with GDPR in Europe, CCPA (and soon CPRA) in California, and other privacy laws in other states, all with their own shades. Data transfers across the borders as well become a point of compliance: e.g., in a case when the data of the wearable of a European user lands on U.S. servers, such provisions as GDPR transfer limitations and such a tool as Standard Contractual Clause are applicable. Legal experts have observed the challenges in finding a balance between opposing privacy principles and have sought to harmonize the principles so as not to have disparate protection and enforcement of wearable data across all nations [8, 18]. Winter and Davidson believe that existing regulatory regimes should be balanced in light of the international character of patient-generated health data flows.

Healthcare and Medical Devices: On top of the general data privacy laws, the wearable with Health capabilities can evoke healthcare-specific laws. The first is whether a particular wearable will be considered a medical device according to applicable legislation. Medical Devices Regulation 2017/745 (implemented in 2021) of the EU [19] welcomed medical devices into the scope of the definition to cover some software and algorithms with medical applications. A consumer-fitness tracker that is sold as a wellness-only product (e.g., counting steps, overall wellness) would not be considered a regulated medical device, but a product purporting to diagnose, treat, or monitor an illness or ailment might be subject to MDR or U.S. FDA medical device regulation. Certain wearables, like a smartwatch with an ECG or a blood oxygen sensor, have pursued and received regulatory approval as a medical device. In the case of Apple and Fitbit, the ECG capabilities of the devices needed to be reviewed by the FDA to detect arrhythmia. When a wearable can be a medical device, it must also comply with medical device safety and efficacy regulations. This covers design controls, clinical assessment, and quality manufacturing practices, and post-market surveillance required by regulators. In this respect compliance refers to not only data protection but to accurate and reliable measurements of the device to be used in medicine. Even in 2021, an international panel of sport and medical professionals recommended global standards of the accuracy and data quality of wearable devices [20]. They highlighted that lack of a standardized system could discard variability of performance of various devices, implying that clinical and privacy compliance would be compromised, and regulators and the industry together would look into benchmarking standards of wearable sensor accuracy.

To avoid the burdensome medical device laws, however, numerous fitness and wellness wearables do not make any medical claims. This brings about an interesting compliance paradox because companies are marketing devices as wellness products, which reduces their regulatory liabilities, but consumers can still use the devices to get health-related information (e.g., using a sleep tracker to detect possible sleep apnea). This is changing the legal liability and compliance implication. Regulators have provided guidance (including guidance on general wellness devices by the U.S. FDA) to define the situations when a product is low-risk and does not need regulation. However, the boundary may be unclear, and there have been those who opine that there should be more regulatory avenues towards high-accuracy consumer health wearables [21]. Devine et al. [22] noted that regulatory perspectives are evolving to accommodate digital health technologies in clinical research and care, suggesting more flexible, risk-based approaches to regulating wearables used in medicinal product development.

Consumer Protection and Product Liability: The other area of law is the general consumer protection law and harm liability. When a wearable device or its companion app offers health-related advice or information (such as notifying a user that their heart rate is potentially dangerous), misleading information might be disastrous. Although not data privacy related, this increases compliance in the area of truth-in-advertising and product safety. Manufacturers should be keen in the way they make the claims, and they should adhere to advertising rules (not exaggerating the health benefits of a device or its accuracy). Also, data security is being considered more as a protection practice to consumers; regulators, such as the U.S. Federal Trade Commission (FTC) have taken action against businesses that have not adopted reasonable security as an unfair or deceptive practice. One such case was a settlement by FTC with a computer manufacturer on insecure IoT devices. The same may be relevant to a wearable manufacturer in the case of bad security that results in a data breach of health information of users. Therefore, the adherence to the best practices in cybersecurity is an indirect legal obligation in order to prevent enforcement procedures and lawsuits [23].

Emerging Regulations – AI and Data Sharing: Looking forward, new regulations on the horizon are poised to impact wearables. The EU's proposed Artificial Intelligence Act, for instance, would regulate certain high-risk AI systems, potentially including algorithms used in diagnostic or health-monitoring capacities on wearables [24]. Wearables employing machine learning to detect health anomalies might need to meet transparency, risk management, and human oversight criteria if the AI Act comes into force [24, 25]. Moreover, the Data Act (2022), which the EU is currently finalizing, is designed to deliver justices in the process of data sharing in IoT among the interested parties. It would expand access rights of users to data created by their IoT devices and require manufacturers to promote data portability and sharing, under some conditions. In the example of wearable compliance, it can mean that businesses must allow users to move their raw health data or share it with third-party services in a format that can be utilized without any loss of privacy. The preference to user empowerment and interoperability that is emphasized in such a law is highly applicable in the situation with medical IoT ecosystems.

International and Ethical Governance: On the international

level, the digital health governance has its origins with the adoption of such international organizations as the World Health Organization (WHO). Even though it is not a sentinel, the ethics and governance of AI in health proposed by WHO (2021) advances values applicable to wearables, such as the notions of inclusiveness, privacy, and responsibility. It means that businesses that have adopted digital health tools ensure that they can adhere to ethical standards, as well as the legal ones. Moreover, it has been argued that WHO or other global organizations need to intervene and help to control wearable health technology on a global scale. Bouderhem [24] stated that since there is a global adoption of E-health wearables, and international jurisdictions have legal gaps, international organizations, such as WHO (with its constitutional mandate in the health field), may be involved in establishing international standards or model regulations. While this is still a forward-looking idea, it highlights that compliance is not only a national or regional issue but a global one in need of cooperative solutions.

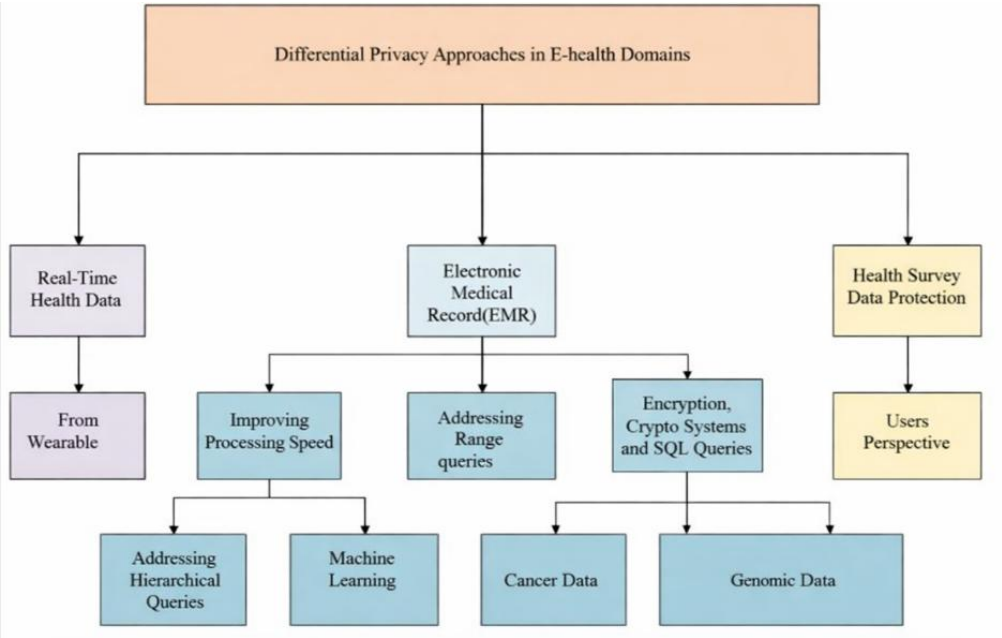


**Figure 1.** Different privacy approaches in the E-health domain

The different privacy approaches in the E-health domain are depicted in Figure 1. The legal and regulatory environment for wearable IoT devices is multi-layered and still evolving. The main compliance considerations are: meeting the strict data protection laws (such as GDPR) by getting the consent of valid users and protecting personal data; addressing the gaps where the consumer health data is not regulated by the traditional health privacy laws (as in the U.S.) and looking forward to new privacy regulations at state or nationwide levels; whether the wearable is defined as a medical device and whether it is safe and effective (and, in that case), complying with the medical device regulations; and complying with the emerging requirements related to AI and data sharing that will continue to affect wearables. The following section will address the operational and practical issues of addressing such legal requirements because merely the availability of laws on books does not mean that compliance is an easy task in the context of wearable technology.

## 3. CHALLENGES IN COMPLIANCE

While the legal frameworks described above establish what is required for compliance, wearable IoT companies and stakeholders face numerous challenges in actually achieving those requirements. These issues are due to technical constraints, business operations, human aspects, and the rapid change of technology and regulation. This part outlines and discusses key compliance issues that traverse legal, technical, and ethical aspects.

1. Data Over-Collection vs. Minimization: Minimizing wearable data practices is one of the core problems, as it is necessary to align the practice with the principle of data minimization. Practically, most wearables have much more data being collected than is necessary to support their primary functionality [7]. As an example, a fitness tracker application can scan location data, address book, or ambient data and fitness data, which could be used secondarily, such as targeted advertising. Ioannidou and Sklavos discovered that a number of the trendy fitness trackers broadcast substantial amounts of personal data (including non-fitness related data) back to the servers, adding to network overhead and privacy risk. Such a tendency to over-collect data contradicts such regulations as GDPR that require collecting only sufficient and relevant data to be used in particular purposes. The dilemma is partially business-motivated - companies would find personal information useful in analytics or collaborations, and partially lacks clarity of purpose (developers may log additional data in case it could be valuable later). The high rate of data generation by wearables makes it difficult to implement stringent minimization; it is difficult to determine in real-time what is and is not to be stored or uploaded without being disciplined in design and at times losing possible business insights. Organizations find it hard to perform comprehensive Data Protection Impact Assessments (DPIAs) and to defend every piece of data that they are gathering with time as new sensors or capabilities are introduced.

2. Minimizing the risk of Informed Consent and

Transparency: It is still an issue to obtain meaningful user consent for wearable data practices. Consent forms or app privacy policies are frequently long, legalistic, and fixed - but wearables have complicated data flows and may have sensitive inferences (e.g., health condition detection). These policies are often read and poorly understood by the users. The overall low interaction with privacy notices is supported by the fact that research shows that users regularly do not read the terms of use of apps or devices. The question of the level of informed consent remains even when it is read: policies do not necessarily describe how data can be aggregated or distributed. As an example, a user may agree that his or her fitness information may be used to improve its services without understanding that it may be provided to third-party analytics or insurance companies under that general provision. The other problematic aspect is the ongoing consent; wearable gadgets collect data in the background, but the consent is sometimes acquired at the initial setup. It is difficult to maintain consent in the long term (particularly where additional functionality is added or the use of the data changes). Other frameworks suggest that the app can offer dynamic consent or periodic re-consent, which can be a user experience blocking. Moreover, in the case of some vulnerable groups of people (elderly users, minors using family health trackers, etc.), the concept of informed consent is even more controversial. To conclude, the transition between legal acceptance on paper and actual user comprehension is a long-standing compliance issue, and the inability to do it properly may result in allegations of non-compliance or ethical misconduct [8, 16].

3. Technical Constraints and Security Limitations: Due to often limited processing power, memory, and battery life, the enforcement of a strong security and privacy policy is limited by what wearable devices can have. It is a resource-consuming technical challenge: heavy encryption of data, regular security updates, and advanced access control measures may be intensely resource-demanding. Creators have a trade-off between the performance of their device (battery life, real-time response) and the intensive security provisions. As an illustration, it may be important to encrypt all sensor data on-site and only send encrypted blobs, which ensures confidentiality; however, the encryption step and key management involve additional computation and user actions to establish keys. There are also cases of low-end wearables that previously chose to send data to smartphones or the cloud in plaintext due to simplicity, which is evidently not in line with security expectations of today [10]. The article by Barua et al. is a detailed overview of the security of Bluetooth Low Energy (BLE) in wearables and demonstrates that it is vulnerable to many threats, including eavesdropping, relay attacks, and device impersonation. As they point out, whereas BLE is climate-friendly (hence its widespread use in the wearables environment), the default pairing techniques proved vulnerable, and many wearable manufacturers did not adequately address the weaknesses in these, making the communications susceptible to interception. It is difficult to be sure that devices meet security state of the art (as needed according to GDPR Article 32, say) because devices are limited; whereas failure may lead to breach of data. In 2023, several fitness technology firms experienced a loss of reputation following breach incidents revealing health statistics of users [23]. Security patching is also a problem, as most wearables lack an easy way to update, which presents unpatched devices in the field. This is a technical and organization challenge: it requires the companies to invest in safe design and maintenance, which can add some expenses and time to market in a very competitive industry.

4. Fragmented Data Ecosystems and Third Parties: Wearable devices do not typically exist in a vacuum, but are components of an ecosystem consisting of mobile apps, cloud databases, analytics services and in some cases integrations with healthcare providers. Such fragmentation brings compliance issues in data flow tracking and compliance with the necessary standards by all parties. As a user wears a fitness tracker, it could be transferred to a smartphone app, and then to cloud servers owned by the company the device is associated with, and potentially third-party cloud analytics or cloud storage services. Every handoff is a place of vulnerability or non-adherence unless handled in an appropriate manner through contracts and technical controls. Under laws such as GDPR, the wearable company should make sure that its processors (e.g., cloud service providers) have sufficient protection measures too [7]. Practically, smaller wearable startups can utilize generic cloud services, and they may not be able to enter into an agreement with strict data protection clauses. Furthermore, the integration of third parties (such as a wellness device that lets users connect their data to a nutrition app or a wellness program at work) also comes with some compliance overhead: data that has already been disclosed may not be subject to the original privacy policy, and the user may not know about such forwarding. According to Sifaoui and Eastin, the landscape in which data brokers and secondary data users act is rather murky and exploitative, being mostly beyond the current regulatory framework, with consumers creating health data on the other end [8]. The trends of a user's heart rate can, say, be sold to insurance companies based on the resulting health score without the user even knowing about it. These practices take advantage of compliance loopholes and underscore the difficulty in ensuring end-to-end compliance when data is no longer in the original ecosystem of devices.

5. Global Compliance and Regulatory Uncertainty: Wearable businesses usually have a global market, which implies that they have to meet several regulatory regimes at the same time. Conflicting legal standards may draw compliance in opposite directions. An example is that the GDPR mandates data protection by default and design, and inflicts severe penalties on noncompliance, whereas certain other jurisdictions might mandate less strict but much stricter data localization policies (as exemplified by the regulations of China, which may require keeping the data of local users on local servers). Managing these differences is resource-consuming. Companies may have various data storage and processing plans in the various regions, and this makes system architecture and testing more difficult. Moreover, regulatory definitions may be unclear - what one country may consider as the definition of health data may not encompass wellness information, whereas in another country it may. According to Taka [15], the conceptual challenge of defining health data when quantified-self wearable devices are involved is that seemingly harmless data (number of steps taken, time spent sleeping) may be health data when interpreted within a context. Being of a dynamic nature implies that companies should make the best bet and treat most of the wearable data as sensitive, which not all regulators have made clear. The looming regulations (like the changing AI Act in the EU or the impending federal privacy laws in the U.S.) also make the compliance planning challenging [18, 24]. The issue that companies have to grapple with today is how to build products

that will remain legal in the future, which may impose new requirements such as a mandate to disclose algorithms or portability of data.

6. Human Factors and Organizational Challenges: The most compromised area of compliance is often not technology or law but human behavior, both in users and organizational contexts. On the user end, inadequate security hygiene (e.g., password reuse, misplaced devices without lock protection, etc.) may lead to damage of the data no matter the protection measures that are established. A user may leave their wearable unlocked or their phone unlocked, and an unauthorized user may access their health information. Even though it is not a direct legal violation by the company, it compromises the overall compliance objective of privacy protection. On the organizational level, compliance may be accidentally created by the employees and developers. To give a few examples, engineers may not have privacy training, and may test with real user data unanonymized, or ignore privacy implications when introducing new features. Hughes-Lartey et al. note that the human aspect is one of the most essential vulnerabilities in IoT security; despite the presence of powerful policies, the error or laxity of the employees may result in the breach. Compliance management involves inculcating a privacy and security culture, which is not an easy task, particularly when dealing with a start-up or a product team that is more inclined to innovation and time-to-market.

7. Ethical and Social Issues: There are compliance issues that go beyond formal rules and reach the ethical level. To illustrate, algorithm bias in the interpretation of wearable data is not explicitly governed; however, ethically, it is a compliance issue of fairness. Should one heart rate algorithm not work as effectively with users who are darker-skinned (because light is not absorbed by the skin pigment in the same way due to skin color differences), the device may not accurately present health alerts to some groups, a failure in ethics. To solve this issue, it is necessary to adhere to the new standards in health equity and inclusive design that, although not a direct legal requirement (unless it is a general anti-discrimination law), is being required by regulators and the general population. The other ethical issue is user autonomy - that the users are not merely legally giving consent, but are actually controlling their data. Wearable organizations are under moral pressure to permit data portability (to enable users take their health data elsewhere) and data deletion (to respect the right to be forgotten), even in those jurisdictions where such rights are not yet codified.

## 4. SELECTION CRITERIA AND CLASSIFICATION APPROACH

It had a systematic literature review process, which entailed a keen analysis of compliance concerns within wearable IoT devices in healthcare. In conclusion of the recent trends in the legal, technological, and ethical aspects of wearable health devices, the review has concentrated on articles published within the period between 2020 and 2025.

The inclusion criteria included:

- Research on health monitoring wearables, such as fitness trackers, heart rate watches, and sleep wearables.
- Globally, privacy, data protection, security, regulatory compliance, or ethical concerns work.
- Peer-reviewed journal articles, as well as some of the high-quality conference papers and authoritative industry reports that provide new information (such as regulatory analysis or standards development).
- Publications that are mostly open-access in order to ensure that they are simple to locate and re-use.

The exclusion criteria were:

- Research papers that consider the IoT in general but do not concern wearable health devices.
- Articles, which do not discuss compliance-related issues.
- The same studies that are longer than those that were already included.
- Non-scholarly, lacks adequate methodological rigor.

The academic databases such as IEEE Xplore, PubMed, and Scopus, as well as the general scholarly search engines, were used as the literature search. Among the keywords, there were wearable AND privacy AND health, wearable AND GDPR, wearable IoT AND security, fitness tracker AND regulation, and wearable AND ethics.

We have found out more possible research to start with. The inclusion and exclusion criteria helped us select 66 references that we would examine further. Their names were divided into three:

- Studies on regulations and laws, such as the law on data protection and policy evaluation.
- Think of how to improve systems and security, and
- Study of ethics.

The distribution of the selected sources was balanced in these areas to ensure that every area was covered.

Legal/Regulatory Compliance: This category consists of all the problems associated with laws, rules, and governance regarding wearable data. Such topics as data protection regulation (GDPR and analogs), health privacy regulation (such as HIPAA), certification of medical devices, the regulation on cross-border data transfer, and new legal requirements (AI regulations, data sharing requirements) are among the main ones. Any literature that was put under this category was a literature that was discussing legal analysis or policy implications of wearables. To illustrate this point, the articles that mention the implementation of GDPR to fitness trackers, or regulatory gaps in digital health, were added to this list. Analyzing these sources together, one can talk about the fullness of the legislation that guarantees the safety of wearables and any uncertainties and uncertainties.

Technical Compliance: This category includes the technological and security dimensions of compliance, that is, how to provide the necessary protection and safeguarding of wearable systems. We added the research on security threats to wearables, privacy-preserving system architecture, methods of data encryption and access control of IoT health data, and such concepts as Privacy by Design in the development of devices. Literature that proposes frameworks or algorithms to enhance privacy/security of wearable data (for instance, edge computing approaches to keep data local [26] or blockchain solutions for data integrity [24, 27]) fall into this group. Grouping these together allows us to evaluate the state of technology in meeting compliance goals such as data confidentiality, integrity, and availability, as well as user data rights (like deletion or portability from a technical perspective).

**Table 1.** Comparative analysis of wearable and medical IoT data ecosystems, highlighting data types, sensing modalities, security and cryptographic techniques, storage architectures, and machine learning approaches, with corresponding benefits and limitations

| Medical Data Collected | Sensors Used | Security / Crypto | Data Storage Method | ML / AI Methods | Advantages | Disadvantages / Challenges |
|---|---|---|---|---|---|---|
| Continuous glucose (blood sugar) [11] | Continuous Glucose Monitors (CGMs) | – | Vendor apps (no EHR integration) | – | Real-time glucose monitoring; reduces hypo/ hyperglycaemia | Data fragmentation; no EHR integration standards |
| Skin conductance, heart rate, body temperature, sweat glucose/ ions [4] | Wearable skin biosensors (Electrochemical, Optical) | – | Wireless (Bluetooth) to smartphone/ PC | Neural networks (ANNs) | Real-time personalized monitoring | Power and HCI limits; communication/ security concerns |
| N/ A (general IoT context) | N/ A | Lightweight ciphers (e.g., PRESENT, SIMON, SPECK) [28] | N/ A | – | Suitable for resource-constrained devices | Security vs. performance trade-offs in constrained devices |
| Heart rate, activity/ location data [29] | Smartwatches (Accelerometer, PhotoPlethysmoGraphy (PPG), Heart Rate sensors) | AES, PRESENT, RSA, ECC, SHA | Over Internet/ Bluetooth to server | – | Enables health tracking and context awareness | Limited device size/ energy restricts use of strong crypto |
| Heart rate, steps, blood pressure, glucose (typical health metrics) [29] | Wearables with Bluetooth Low Energy (BLE) (Fitness trackers, Heart Rate monitors) | AES-CCM (used in BLE) | Via mobile app/ cloud | – | Low-power communication; ubiquitous BLE use | BLE vulnerabilities (insecure encryption, MITM attacks) |
| Sensitive patient health data | N/ A | LWC algorithms (AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, RECTANGLE) [30] | IoT device storage (16KB–2MB files) | ML models for performance evaluation | Identifies efficient encryption (e.g., RECTANGLE) | Balancing encryption speed, energy, memory usage |
| Asthma level, blood pressure, ECG, body temperature [31] | Wearable health monitors (Electrocardiogram (ECG) patches, Blood Pressure (BP) cuffs) | PUF-based authentication; hash/ symmetric keys | Mobile app → cloud | – | Lightweight, privacy-preserving auth; group-proof authentication | Insecure wireless channels; need for lightweight yet secure auth |
| Insulin pump settings (delivery rate) [32] | Implantable insulin pump | – | – | – | – | Cyber-vulnerability: hackers could reprogram pump remotely |
| PPG signals (heart/ breathing rate), EDA, motion gestures [33] | Wearable sensors (PhotoPlethysmoGraphy (PPG), ElectroDermal Activity (EDA), Accelerometer) | – | Publicly shared dataset | Siamese CNN (multi-modal) | – | Privacy risk: 71% re-identification from "anonymized" sensor data |
| Epileptic seizure signals (EEG, vitals) [34] | Wearable Epilepsy monitoring devices | Federated Learning (privacy-preserving) | Edge devices + Cloud (AWS) | Federated ML models (distributed learning) | Privacy-preserving distributed analytics | Limited compute/ comm/ battery on wearables |
| Vital signs (heart rate, BP, glucose) [35] | Wearable devices (Fitness trackers, CGMs, ECG patches, BP cuffs) | Blockchain ledger (decentralized, encrypted) | Blockchain (distributed storage) | – | Tamper-proof data storage; patient-controlled sharing | Lack of standards/ interoperability; scalability issues |
| Various clinical sensor readings [36] | Medical Internet of Things (IoMT) devices (Wearables and | Encryption on wireless (HIPAA/ | Cloud/ remote servers | – | Continuous monitoring and remote care | Data theft risk in transit; multiple protocol vulnerabilities |

| | | | | | | |
|---|---|---|---|---|---|---|
| | implants using BLE, Wi-Fi, LoRa) | GDPR compliance) | | | | |
| Wearable health/ activity data (e.g., steps, heart rate) [37] | Consumer wearable devices (smartwatches, fitness trackers) | – | (Data typically flows through device apps or cloud platforms) | – | Passive, continuous data collection with minimal user burden | Challenges in privacy, data quality, digital equity and third-party ethics |
| Various wearable sensor data (physiological, activity) [38] | General wearable sensors (fitness/ activity trackers) | – | – | – | Potential to automate care processes and engage patients through feedback | Multiple sociotechnical issues: data integration, privacy and governance gaps |
| Physiological biometrics (e.g., ECG, motion) [39] | Wearable ECG and motion sensors | – | – | – | – | High re-identification risk: even 1–300 seconds of (deidentified) wearable sensor data can uniquely identify individuals |
| IoMT signals (e.g., heart rate, glucose) [40] | Wearable heart monitors, smart insulin pumps | Adaptive Differential Privacy; lightweight homomorphic encryption | Edge processing (local devices) | Hierarchical federated learning | Local data analysis preserves patient privacy and greatly extends device battery life | Edge device resource limits (compute, energy); regulatory compliance (HIPAA/ GDPR) and system complexity |
| IoMT sensor data [41] | IoMT sensors | Two-phase authentication: ECDH for key exchange; AES-GCM for encryption | – | – | Strong sensor-to-server security with low computational cost; ~45% faster encryption and reduced latency vs. standard methods | Complexity of dual-phase setup (key exchange + encryption) adds design overhead (though authors report minimal impact) |
| Electronic medical data (EHR, device records) [42] | n/a | Post-quantum cryptography (lattice-based, code-based, hash-based, multivariate) | – | – | Quantum-resistant security for future threats | Challenges in adoption: computational overhead, system integration issues, cost and training requirements |

Ethical Compliance: In this category, we will take work on the basis of ethical principles, user perceptions, and social implications of the use of wearable health data. This encompasses research on user privacy issues and attitudes [14, 43], the informed consent user experience, equity and bias in wearable data, and ethical frameworks/guidelines of data management. We categorized literature in this area as literature that concerned what should be done beyond the formal legal mandates such as making algorithms fair or maintaining user autonomy. Empirical studies on the user perception of data sharing or the reasons behind trust in wearables are also included [14, 44], because the latter has direct implications on ethical compliance (e.g., the establishment of trust through transparency in communication with users is ethically responsible). The analysis of these sources together will allow us to formulate the ethical norms that wearable companies should pursue, which usually shape or precondition regulations.

These types are independent of each other but interconnected. As an example, legal compliance requirements (such as the principles of GDPR) affect the technical solutions that must be adopted, and both of them are supported by ethical aspects of privacy and autonomy. Our classification method clearly recognizes overlaps, i.e. a particular reference may fall under several categories, but we still categorize it according to the category which is its main focus. To illustrate, a paper that suggests a privacy model of wearables and also talks about legal gaps would be classified as legal/regulatory, whilst a paper that constructs a new encryption scheme of wearables with a little bit of GDPR would be classified as technical. Table 1 gives a summary of some of the representative issues and example references in each category.

This classification approach guided our literature analysis in Section 6 and Section 7. In Section 6, we specifically address compliance challenges within the wearable IoT context, referencing studies from all three categories as needed (e.g., highlighting technical security flaws alongside legal uncertainties). In Section 7, we review frameworks and solutions proposed in literature, again structured by how they address legal, technical, or ethical aspects of compliance or an integration of these. By organizing the discussion along these lines, readers can clearly see the requirements and best practices in each domain, as well as how they converge towards the common goal of trustworthy wearable health devices.

**Table 2.** Classification of compliance issues in wearable IoT systems, outlining key categories, their focus areas, representative issues, and corresponding references from recent literature (2020–2025)

| Category | Focus | Example Issues/Topics | References (2020–2025) |
|---|---|---|---|
| A. Legal/Regulatory | Laws, regulations, and policy frameworks | GDPR requirements for wearables; HIPAA gaps; MDR for medical-grade wearables; cross-border data; regulatory proposals (AI Act, Data Act) | GDPR & wearables [7, 15]; HIPAA applicability [8, 9]; Reg. gap in digital health [45]; Data governance policy [18] |
| B. Technical | Security and privacy engineering | Data encryption & anonymization on-device; secure communication (BLE security); access control; privacy-by-design architecture (edge computing, blockchain); breach prevention | BLE threat survey [10]; Privacy-by-design frameworks [7, 26]; Blockchain for IoMT security; Access control for health data [11] |
| C. Ethical | Ethical principles, user perspectives | User consent and understanding; trust and privacy concerns; data bias and fairness; user autonomy and control; data sharing attitudes; transparency and accountability beyond legal mandates | User privacy concerns studies [14, 46]; Fairness/equity (skin tone bias) [13]; Ethical frameworks [12]; User data-sharing behavior [1, 47] |

Generally, the literature indicates that regulatory frameworks, types of devices, and the situations of their application differ significantly. Much has been said to establish compliance requirements, and yet there is no single method of implementing these requirements into practice in real-world wearable IoT systems.

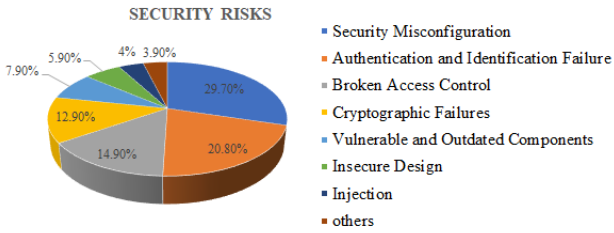


**Figure 2.** Common security risks

The graph in Figure 2 compares the modern system security threats. Security misconfiguration is the greatest risk, and most of the vulnerabilities are authentication and identity failures and failed access control. Systems are also weaker due to cryptographic failures and outdated components. The statistics indicate configuration and access as the largest cybersecurity threats.

## 5. COMPLIANCE CHALLENGES IN WEARABLE IOT

Health monitoring wearable IoT devices have some of the special compliance issues that arise due to the context, form factor, and user interaction models. Continuing on the overall challenges that have been discussed above (Section 4), we move on to discuss challenges within the context of the wearable IoT domain. We also explain them by giving concrete examples of devices that monitor fitness, heart-rate and sleep with references to empirical research and technical examination in the literature.

This part examines how these issues evolve as time passes in the context of wearable IoT. Available literature suggests inconsistency not only between different device types but also between regulatory policies and risks, highlighting the inconsistency in the definition and enforcement of compliance. In this section, the examples of the devices used in fitness, heart-rate monitoring, and sleep monitoring are offered to unite the findings of the real-world studies and technical analyses in order to identify the primary issues, contrast the way they emerge in various scenarios, and indicate the gaps that are still present in the current research.

1. Resource Limitation and Data Security: Wearables are commonly tiny, battery-operated, low-caliber computers. This poses a basic conflict between the requirement of a strong data protection and the capability of the device to enable the same. As an example, the sensor information can be encrypted continuously, which may burn battery and processing power. Most wearables therefore do little processing on the devices themselves but transmit that data to accompanying smartphones or cloud servers to be processed and stored there. Although this architecture is convenient, it would imply that sensitive raw data is on transit very often, exposing it. Devine et al. [22] noted that these logistical aspects make it impossible to install more advanced sensors in wearables as more data is collected (e.g., high-fidelity biosignals to stage sleep), the larger the device and the network, and this can be incompatible with privacy without proper measures. Practically, other manufacturers choose to only send data periodically or sometimes summarily in order to conserve energy, although that may be contrary to user or clinical expectations of access in real-time. The dilemma lies in striking a balance: such techniques as on-device summarization or edge computing can help lower the rate of raw data transmission, and it is not easy to ensure that these procedures do not lead to the loss of data integrity or security.

Furthermore, wearables often lack hardware-based security modules (like secure enclaves) that smartphones have, making them more vulnerable if compromised. Ensuring compliance (e.g., encryption at rest) on a device without secure storage or user authentication (most wearables don't require PIN/password to access) is an open issue.

2. Continuous Monitoring and User Consent: Unlike one-time medical tests, wearables involve continuous data collection, which blurs the boundaries of user consent. Obtaining a one-time consent at app installation may not cover future scenarios, yet constantly interrupting users for consent is impractical. Wearable IoT devices often collect data in the background – during sleep, exercise, etc. – when users are not actively engaging with the device's interface. This raises the challenge of keeping users informed and empowered about ongoing data practices. A compliance issue arises when new insights are derived from aggregated data; users might be unaware that, say, their sleep pattern data over months is being analyzed for mental health indicators. According to a study conducted by Dobson et al. [37], researchers noted that in health research involving consumer wearables, participants were worried about the third party intervention and the use of data after the immediate intention. The wearables are continuous, which implies that purpose creep (using data in ways other than the original purpose) is a fact. As an example,

a fitness site might begin to examine the trends in heart rate to indicate potential health concerns (a value-added service) but this would creep into diagnostic areas that the user did not directly consent to. To ensure compliance in this case, creative consent approaches (possibly tiered consent to various data uses) and explicit opt-out options would be needed, which are not yet a norm in wearable ecosystems.

3. Data Accuracy and Validation (Clinical vs. Consumer Grade): Wearable devices do not always go through the same type of validation that medical devices do. Consequently, their data can be inaccurate or biased. Although accuracy may appear as a device performance problem, it is also a compliance problem in cases where the wrong data may misguide the users or healthcare providers. In case a wearable indicates that a user is stressed due to his or her heart rate variability, but this is not really the case, and rather a sensor error, the user may make unnecessary medical decisions. Compliance wise, the misleading health information may be regarded as a breach of consumer protection laws or even health laws in case of harm. Also, the fact that some groups are more prone to data inaccuracies (e.g., skin-tone based bias in optical heart rate sensors) relates to ethical compliance in terms of fairness. Colvonen et al. [13] emphasized the fact that even popular wearables could be much less precise when used by people with darker skin, but this fact had not been publicly revealed and discussed by the manufacturers. The compliance issue is that there is no existing legislation that specifically states that your wearable should be equally good across all skin tones, but it is an ethical requirement and is becoming a regulatory interest issue (such as the FDA is currently examining the performance of demographic subgroups in device submissions) that is vital. Manufacturers are under pressure to test their devices in various populations and use environments. Compliance may therefore be achieved by following new standards (IEEE or ISO could come up with standards on the accuracy of wearable sensors) and being open about the limitations of the devices. Ash et al. [20] recommend the creation of global standards of wearable accuracy and data quality to facilitate their application in sports and medicine. Until these standards become more commonly used, the difference between wearable consumer performance and clinical-grade expectations is one area of compliance grayness.

4. Interoperability and Data Integration Issues: One of the biggest promises of health wearables is that it can be integrated with electronic health records (EHRs) and clinical workflows, allowing doctors to use patient-generated data in care. Nonetheless, the incorporation of wearable data into healthcare systems creates compliance challenges regarding the standardization, provenance, and liability of data. According to Espinoza et al. [11], one of the obstacles to the integration of continuous glucose monitor (CGM) data (a form of wearable) into EHRs is the absence of data standards. Analogically, most fitness and wellness wearables store data in proprietary data formats; upon data transfer to clinicians, the risk of misinterpretation is high. In compliance terms, in the event that wearable data is used to make health decisions, it will be important to make sure that the data is of a specific quality and format. It also raises the question of whether healthcare providers are liable (according to such laws as HIPAA or medical malpractice standards) to act on wearable data. Should a patient provide a doctor with his/her sleep tracker data, is the doctor required to review it or confirm its accuracy? These uncertainties have made patient-generated data to still be suspicious to many clinicians today. On the patient end, the absence of smooth interoperability may result in insecure workarounds, such as patients exporting data to spreadsheets or third-party applications to share with physicians, which may be a compliance violation in the event that such sharing is not done with the required safety measures. The difficulty is the development of interoperable but secure wearable data exchange pipelines. Some attempts such as IEEE 1752 Open Wearables or HL7 FHIR-based wellness data APIs are underway, but they are not widely used. Up to this point, integration can be based on ad-hoc solutions, which may not be fully adhering to health IT security or privacy requirements.

5. Multistakeholder Data Governance: Wearable data is often of interest to a variety of actors: the user, the device maker, the app developers, the researchers, the healthcare provider, the insurers, even the employer (in wellness programs). It is extremely complicated to control access and administration of who is allowed to access what data. As an example, one can take an employer-sponsored wellness program in which the employees wear fitness trackers to receive insurance rebates. The employer may just be allowed to receive aggregated activity scores (due to privacy), yet the insurer may need some personal information to compute rewards, and the device company continues to gather detailed metrics. It is difficult to make sure that every stakeholder can only access data as agreed by the user. Cases of programs in which wearable data was accidentally shared with other people other than intended recipients because of API settings or misconceptions and resulted in privacy breaches have occurred. In addition, in case an insurer makes decisions based on wearable data (such as premium adjustments), it also brings up legal and ethical concerns regarding discrimination and privacy.

6. Contextual Privacy Expectations: Wearable devices have a tendency to record information in places that are regarded by users as private (sleeping in his or her bedroom, etc.). When such data is distributed or used in a manner that the user had not anticipated, it may result in a tremendous backlash of privacy, even though it may not be illegal. This is an issue of satisfying contextual privacy expectations - a notion in which the perception of users regarding what will be done with their data should correspond with reality to comply (particularly with laws such as GDPR that focus on fair and transparent processing). To illustrate, one user may be okay with their heart rate data being used to display fitness trends on their app, but not okay with the same being sold to third-party marketers to market stress-reduction products to them. The scenario has changed to commercial marketing rather than personal wellness, which is against expectations. Taka [15] stated that health data definition can be relative to the context of a given instance, e.g., data on heart rate as given by a cardiologist and as given by a sports app can be perceived differently under the law. However, in the eyes of the user, it is also contextual, such as the difference between providing friends with step counts to a social leaderboard and providing them with actual GPS tracks of runs, which may be considered as intrusive. Wearable platforms are not able to offer such finely-tuned privacy options that can appeal to these refined tastes. Very often it is either share or not share as opposed to more sophisticated options. Due to this, firms can over share information on accident, thus violating the contextual norms. Adherence to the principle of contextual integrity (a privacy theory of Nissenbaum [48]) is not legally obligatory, but it follows the

zeitgeist of numerous rules that require fairness.

The wearables used in clinical settings and dealing with physiological data are under stricter regulatory and ethical control compared to the fitness-related devices. This demonstrates that the compliance requirements change depending on the sensitivity of the data.

Wearables that process physiological information in a clinical-grade are more prone to regulatory and ethical scrutiny compared to fitness-oriented devices. This indicates that the compliance requirements differ depending on the sensitivity of the data. One of the biggest differences between jurisdictions is the level of cooperation between them in terms of regulations. There are those that are well-structured and those that are more sector-based.

## 6. COMPLIANCE FRAMEWORKS AND SOLUTIONS

The complex compliance issues described above should be tackled with elaborate frameworks and novel solutions. Researchers, industry consortia and policymakers have in recent years suggested a number of ways to improve legal, technical and ethical compliance of wearable IoT devices. The following section draws attention to significant frameworks and solutions, but organizes them based on their main focus (however, many of them share common advantages).

1. Privacy and Security by Design Frameworks: It is one of the major strategies to provide privacy and security concerns into the wearable devices and systems design stage, which is commonly referred to as Privacy by Design (PbD) and Security by Design. In GDPR and other laws, data protection by design is a compliance standard in place. This practically implies that the engineers should design in advance the way data flows will be reduced, secured, and regulated. Models have been created in order to curb this process. To provide an example, the systematic review by Özacağdavul [7] proposes essential design measures, including data encryption, anonymization, and limited access control, as the key to achieving GDPR compliance in wearables. A suggested framework that comes out of that analysis would be to apply the edge computing to data processing - i.e., to process health data on the device or phone itself as much as possible and only send required results to the cloud. This method can greatly minimize exposure and ease compliance (because less personal data is exposed to the personal area network of the user) by making the raw data available locally (and directly under the control of the user). Said et al. [26] used a prototype IoT architecture to integrate edge computing with encryption to meet the requirements of both the HIPAA and GDPR in a healthcare monitoring context. In their design, data that is sensitive is handled on a gateway (such as a smartphone) that applies consent policies, encrypts data, and uploads to cloud servers such that plaintext personal data never reaches cloud storage. Such architectures are in line with the principles of PbD, and they essentially create compliance in the structure of the system.

Security-wise, platforms such as the Platform Security Architecture (PSA) of IoT by ARM or IEEE best practices have been implemented on the wearable. According to Barua et al. [10], they suggest a robust security architecture that involves device authentication (to eliminate unauthorized wearables) and end-to-end encryption of data transmission, as well as periodic updates to the over-the-air to address vulnerabilities. Secure communication is also currently a standard practice within many wearable companies (e.g., secure connection via Bluetooth LE, secure connection and encryption) to safeguard in-flight data. Some have also added hardware security enclaves in more recent smartwatches to store encryption keys or do cryptographic operations without secrets being visible to the operating system. Such technical measures are included in a bigger scheme of providing adherence to the state of the art in security, as the regulation requires.

2. Data Governance and Consent Management Solutions: In order to address the issue of user consent and data management within an ecosystem, solution frameworks have been developed with the emphasis on user-centric data management. The first one is the development of personal data stores or vaults that contain all the wearable data of a user under their control, and the user has the ability to grant third parties permissions. Although it remains a developing concept, it echoes the notion of users being the owners of their data and giving time-limited or purpose-limited access. An example would be a user having a personal health record application which operates by retrieving the information in their fitness tracker, sleep sensor, etc., and then generating an information report that could be shared with a doctor visit without the wearable company sharing the data itself with the doctor. This way, compliance with privacy is enhanced by involving the user in every transfer. Some research prototypes and commercial startups (e.g., using blockchain-backed personal health records) are experimenting with this model.

3. Anonymization and Aggregation Techniques: To address data privacy while preserving some utility, researchers have developed techniques to anonymize or aggregate wearable data. One practical solution for compliance is on-device data anonymization – for instance, stripping identifiers and reducing granularity of certain data before uploading. Chikwetu et al. [49] evaluated methods of de-identifying wearable data and warned that naive de-identification can give a false sense of security. They discovered that with the removal of obvious identifiers, even granular sensor data (such as fine-grained GPS logs or activity history) can tend to re-identify an individual or disclose sensitive patterns. Thus, some more sophisticated methods, such as differential privacy and k-anonymity have been proposed. Differential privacy may enable businesses to publish or analyze population-level information about wearable users (to do research or to serve the public health) with mathematical assurances that no individual data can be identified. Differential privacy has been applied in some health studies that were conducted by some of the largest tech companies, such as aggregating the number of steps that millions of people took to identify trends without revealing any personal information of an individual. When incorporated into wearable data platforms, these techniques would serve as compliance tools because they reduce risk associated with using data outside the main user-facing services.

4. Blockchain and Distributed Ledger Solutions: It has been suggested to implement blockchain as a solution to improve the compliance of IoT including wearables, primarily through generating transparent and tamper-evident data records on data transactions and user consents. Ghadi et al. [35] have shown an Internet of Medicine Things (IoMT) security blockchain-based system. Data provided by wearables, in their implementation, is stored in a blockchain ledger that is available to stakeholders (user, healthcare provider, etc.) with relevant permissions. The blockchain can provide an

unalterable history of who accessed data and when, which would be of great assistance in compliance audits. As an illustration, by the user rescinding consent, the event will be recorded, and any further access by a third party will be blocked or marked through smart contract logic. The decentralization of blockchain may also facilitate interoperability - various entities (hospitals, insurers) may rely on the common ledger to ensure the integrity of data without the need to have a single central party to control it. Ghadi et al. [35] concluded that the introduction of blockchain could be used to address such requirements as data integrity, accountability, and even some of the standards, such as the audit trail and access control requirements, provided by HIPAA. Nevertheless, they also described the performance and scalability aspects; therefore, these solutions could initially be implemented in small areas (e.g., a group of healthcare providers exchanging data as a part of an accepted wearable initiative). Figure 3 depicts a Blockchain-enabled smart healthcare architecture that integrates data with device connections with heterogeneous applications.

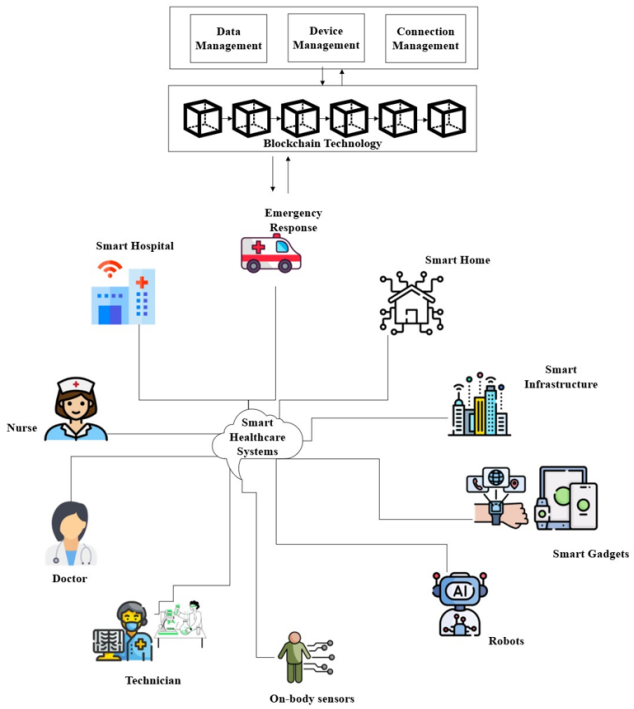


**Figure 3.** Blockchain-enabled smart healthcare architecture

5. Standards and Certification Programs: An emerging approach to foster compliance is developing standards and certification for wearable devices regarding privacy/security. Analogous to how medical devices have FDA clearance or CE marking, there are calls for privacy certification of consumer health tech. For instance, the ISO/IEC 27701:2019 standard (Privacy Information Management) or the NIST Privacy Framework (2020) could be adopted by wearable manufacturers to structure their compliance programs. Some companies have begun voluntary compliance with standards like ISO 27001 (information security management) to demonstrate commitment to data security. Additionally, industry coalitions are creating codes of conduct – in Europe, a "Code of Conduct on privacy for mHealth apps" has been proposed to give guidance to health app and device developers on how to comply with GDPR in practice. Compliance with such a code can be used as mitigating evidence.

6. User Education and Engagement: User education is not a technical framework, but as a solution to compliance, it is brought up in various studies as being very important. The more users know about the type of data their device is collecting and have control over it, the more they can behave in a way that supports compliance (e.g., modifying the privacy settings, locking down their device, etc.). Privacy dashboards have been introduced by some wearable platforms - such as a central spot in the app where users can view all the data of all the data being gathered and switch on permissions. This is in line with the transparency provisions of GDPR and provides the user with a feeling of control. According to Dobson et al. [37], researchers involving wearables in research should ensure that their participants are given appropriate education regarding the flow of device data and privacy, which may also be relevant to commercial implementations. Essentially, treating user awareness as part of the compliance solution set can lead to a more trusting user base and potentially fewer complaints or issues. The benefits of data privacy risk assessment are described in Figure 4.

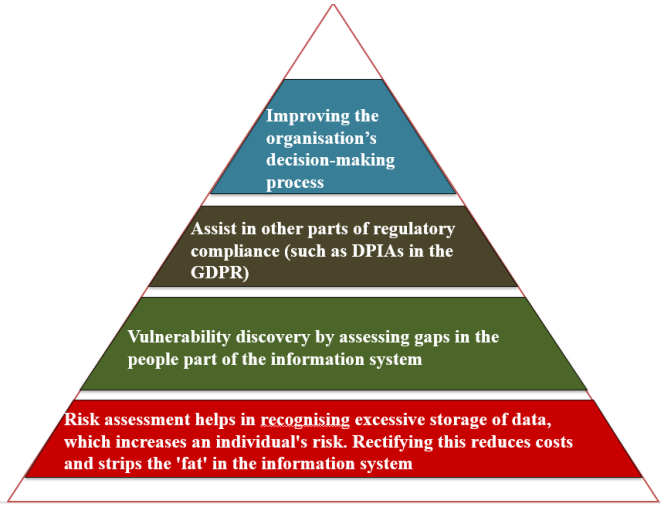


**Figure 4.** Benefits of data privacy risk assessment

## 7. OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Although much has been done in terms of comprehending and responding to compliance concerns of wearable IoT health gadgets, there are still a number of unresolved problems. With the changes in technology and data practices, the legal framework and technical protection have to change. In this final section, we identify some of the main areas that require further research, innovation, and development of policies, and propose future directions that may improve the compliance of wearable health technologies.

1. Balancing Global Regulations and Standards: One of the challenges being immediately important is the harmonization of regulations. The wearable devices are sold worldwide, and the level of compliance is still mostly country/region-based. This division causes ambiguity and excessively high compliance overhead. International discussions should be made to come up with minimum standards of wearable health data protection. The potential path forward is to create a global system of compliance of consumer health data, potentially managed by bodies such as the International Medical Device Regulators Forum (IMDRF) or WHO. Bouderhem [24]

supported the idea that the WHO may lead in the international regulation of E-health wearables, using its international health mandate. Although the guidelines provided by WHO (e.g., 2021 AI ethics guidelines) are not binding, they may impact national policies. The next stage can be model regulations or mutual recognition agreements so that a device that is compliant in one significant jurisdiction (e.g., GDPR and MDR in EU) is mostly considered to be compliant in other jurisdictions with few local modifications. Also, the creation of a certification that is recognized worldwide (similar to CE/FDA but regarding privacy/security) may be a breakthrough. This would enable consumers to find it easy to identify devices with high compliance standards, regardless of the location where they are manufactured. Harmonization is politically difficult, but there is a chance with the wave of privacy law adoption around the world (more than 100 countries now have data protection laws) that harmonization will be achieved with wearables in particular.

2. Context-Aware and Adaptive Privacies: According to the observations, wearables work within dynamic settings and generate diverse kinds of data. Existing consent and privacy systems are more or less fixed. There is a need to research on adaptive privacy management systems in future, which can automatically adapt data handling depending on the context and preferences of the user. As an example, a wearable could be context-aware and, upon noticing that the user is somewhere sensitive (such as home during personal time), restrict data transmission, or vice versa, when in a medical check-up mode, provide a healthcare provider with more data to its system. Machine learning may be used to study the privacy comfort zones of a user and then actively enforce them. Such smart privacy can take it a notch higher than merely seeking user input and help them in real time. It will be essential to ensure that these systems are transparent and can be controlled by the users as an override (to prevent paternalism). It is at the convergence of human-computer interaction (HCI) and privacy research on how to create privacy tools that are effective and easy to use on small wearable interfaces or on companion applications. It is a direction of the future that can give power to users and enhance ethical compliance, making the behavior of devices closer to the expectations of the users.

3. Solving Algorithmic Bias and Fairness: The problem of bias in wearable data analytics is an unresolved problem that needs further investigation and potentially regulation. Research such as Colvonen et al. [13] has highlighted racial bias in device accuracy, and other groups (e.g., women vs men in some measures, or older adults with different physiology) could also have such disparities. The next step in work should be algorithmic responsibility in wearables: the creation of testing procedures to assess the work of the device in various groups of users and the development of corrective algorithms or calibration procedures. A possible future trend is that regulatory authorities will include fairness audits in the process of approving or certifying devices. As an example, the FDA might demand that a new health wearable has been tested on a demographically diverse sample and that any performance differences are reported or addressed. On the research front, wearable sensing should be subjected to AI fairness literature methods (such as re-sampling, personalized calibration models, or multi-spectral sensor methods to address skin-tone bias). Fairness is not only ethically necessary but also relevant to compliance in the long term - anti-discrimination laws may be invoked in the future in case some groups are systematically disadvantaged by the operation of a device. To address this challenge, an interdisciplinary approach (including data scientists, clinicians, ethicists) is required to make wearables beneficial to all populations equally.

4. Governance of Longitudinal and Secondary Data Use: Since wearables are used over time, the longitudinal data they generate can be used to unlock valuable insights (to personal health or research), but also creates new compliance issues. A device can accumulate information that is highly personal over time, trends that can be used to predict health status, behavioral tendencies, even mood or mental health status. The future regulations might have to be more specific on secondary use of long-term collected data. As an illustration, when a company that gathered fitness data to give user feedback in the future intends to use it to train a machine learning model to detect diseases, is the initial consent adequate? Probably not under GDPR (which demands compatible purpose), but it is interpreted differently. One direction that is being considered is to set up clear guidelines or industry codes of secondary use: it may be necessary to re-consent to any further use beyond a specific scope, or to anonymize the data after a time unless the user re-consents. Technologically, they should develop tools to safely share longitudinal wearable data to research - such as federated learning where data remains on the device and only model updates are exchanged may enable useful research on wearables (e.g., collective health trend analysis) without violating individual privacy. Federated learning has already demonstrated itself as a promising approach to training AI models on distributed health data with privacy constraints. Federated learning networks could be studied in the context of wearables, where wearables are involved in collaborative analysis with privacy guarantees. This would be consistent with compliance by design, allowing useful secondary applications (such as epidemiological studies) with minimal exposure of raw data [34, 50].

5. User Literacy and Engagement Strategies: This is a slightly softer, yet important, future direction of enhancing digital health literacy in terms of wearables. With such devices becoming commonplace, people must know not only how to check their number of steps, but also what happens when their data is shared. Finding methods of educating users in large scale is an open challenge. It may be considered in the form of gamification or incentive-based learning in apps (e.g., a privacy badge after following a tutorial on how to manage your data, or a real-life reward upon choosing a privacy-friendly setting). Active and aware users may serve as a check and balance to business - when they are aware of their rights and tools, they will be inclined to request compliance and alert about problems. Better regulations can also be pushed in the long term by increasing public awareness since informed consumers will pressure industry and regulators to seal gaps. In academic terms, therefore, the consideration of various communication strategies (icons, labels, interactive privacy settings) to present complex information in a concise manner on the mobile/wearable platform is a relevant research topic [51, 52].

6. Real-world Compliance Monitoring and Auditing: There will also be enhanced mechanisms of monitoring and auditing wearable data practices, which will enhance future compliance. At the moment, regulators have a problem with auditing an infinite number of apps and wearables. Automated compliance auditing software might be one option: e.g., software capable of scanning the network traffic of an app to determine whether

it is covertly transmitting data to third parties without informing them or analyzing firmware to determine whether it is being used to encrypt data. In this area (privacy tech auditing), the research may increase regulatory supervision. Also, user data transparency tools such as personal data records (such as access logs in medical portals) may become the norm. Certain fitness platforms already enable their users to access their data; it would be more accountable to expand to an audit record of who/what has accessed their data. This is also related to blockchain solutions, however, even less complex server-side logging, which is visible to the user, may be useful. The difficulty lies in the process of making these logs readable and not daunting. In the future, AI assistants that summarize such data as your data was accessed X times this month by Y services, all within the scope you allowed may be integrated into work.

Although much research has been conducted, there are still some gaps, such as the lack of global standards, insufficient adoption of privacy-by-design on resource-constrained devices, and insufficient focus on equity and transparency in wearable data analytics.

## 8. ENCRYPTION AND AUTHENTICATION FOR COMPLIANCE IN WEARABLE IOT HEALTH DEVICES

Wearable health devices produce very sensitive personal information, and therefore it is vital to ensure that the data is strongly encrypted and authenticated to comply with the law and provide privacy to patients. Some laws such as GDPR in the EU and the HIPAA in the US mandate organizations to deploy security controls that are reasonably suitable (e.g., encryption of data, access control) in order to protect health data [7, 40]. The EU Medical Device Regulation (MDR) also serves to ensure that manufacturers design devices that are resistant to unauthorized access to guarantee the safety of the patients [53]. This seriously implies that wearable IoT health devices will have to ensure the confidentiality and integrity of data at rest (on the device or phone) and in transit (to cloud servers or other systems) by means of strong cryptographic tools as well as regulate access by user and device authentication.

Standardized Cryptographic Techniques: Symmetric encryption (e.g., AES) is used in wearable devices as the most effective data encryption technique because of limited resources. Symmetric ciphers are also fast and small thus suitable in protection of realtime sensor data in wearables [29, 54]. Asymmetric cryptography (RSA, ECC) is normally reserved to secure key exchange and digital signatures as it is more computationally intensive [55]. An example of this is the use of an initial Elliptic Curve Diffie Hellman handshake with a smartphone by a device to create a shared secret key and then encryption of health data streams with AES-256. Such methods are integrated in standard protocols such as Bluetooth Low Energy and TLS to offer encrypted communication channels. Authentication is provided to prevent unauthorized access to data: wearable-to-phone pairing is frequently based on secret PINs or passkeys, and devices/users are authenticated with a token or a certificate by the backend servers. Multi-factor authentication (e.g., wearable is only paired when a user confirms in an app) helps to enhance security even more. It has been found that more sophisticated two-phase authentication protocols can achieve a substantial decrease in overhead one study found that an intelligent dual-authentication Asif et al. [41] demonstrated that the proposed two-phase dual authentication framework significantly improved performance, reducing encryption/decryption time by over 45% and latency by 28.42% compared to conventional approaches [41]. In summary, the most advanced wearables use a mixture of confidentiality encryption and access control authentication procedures, which comply with the privacy law security principles.

Regulatory Expectations and Data Governance: Global regulation of data protection laws clearly or unspoken require wearable health data to be encrypted and be under access control. An example of Privacy by Design and data minimization (practiced by GDPR, which advises against misuse of data collected by wearables) is that wearables must not gather more data than is essential and should secure (usually through encryption/pseudonymization) the information they do. Article 32 of GDPR stipulates that organizations ought to evaluate risks and take certain actions such as encryption to enhance a reasonable degree of security [36]. When a wearable device sends personal health data without encryption or without appropriate consent, it will put the wearable at risk of breaching GDPR and attracting fines (up to 4% of the global revenue). Similarly, the Security Rule of HIPAA requires protection of electronic protected health information; it does not dictate the type of algorithms to use, but in effect, it requires the encryption of health data both when at rest and in motion unless it is replaced with an equivalent control. Specifically, edge computing and strong encryption have been suggested as part of the healthcare IoT designs to meet the requirements of GDPR and HIPAA at the same time. The Cybersecurity is also elevated by the EU MDR (Regulation 2017/745) that partially became effective in 2021: the manufacturers are obliged to make sure that the medical IoT devices do not have any unacceptable risks, including the data security risks, throughout the product lifecycle. It is interesting to note that regulators such as the FDA have started to publish cybersecurity guidance, and even deny or recall devices which fail to meet minimum security. To guarantee compliance, it follows that wearable IoT companies must design their products to apply end-to-end encryption, strong identity management and stringent data governance policies (including consent, storage and sharing). As an example, information must be encrypted on the device and it must be encrypted on the cloud repositories, and only authorized health practitioners or the user can decrypt it. Moreover, accountability is expected as the audit trails and key management procedures should be in line with standards (ISO 27701, NIST cybersecurity framework, etc.). To conclude, regulatory frameworks are currently anticipating encryption and authentication as not optional benefits of a health IoT system that handles personal data but as standard functions.

Difficulties with Implementation: Strong crypto on wearables has a number of difficulties to implement despite the obvious advantages.

The major concern is the resource constraints, a lot of wearables are battery-powered with low-power microcontrollers. The complicated encryption or handshakes can strain the small CPU, memory and energy budget, reducing the performance or battery life of devices. An example is asymmetric cryptography or very long key lengths which may be inconvenient to execute on a fitness tracker. In a 2022 review, it was observed that IoT health devices can frequently not support the use of complex encryption and

authentication schemes due to substantial computation and latency penalties, which may disrupt the real-time use of the device.

Another problem is device interoperability, i.e. wearables should be able to communicate with smartphones, cloud APIs, and even with other IoT devices. When each has various proprietary encryption protocols, they are hard to integrate. The absence of common frameworks on IoT security provides a reason to sometimes resort to insecure approaches by manufacturers in the name of compatibility [56]. Some wearables used to send health data in plaintext or hard-coded weak keys just to make it easier to share data, which would not pass as green in the context of GDPR and HIPAA nowadays. In fact, research indicates that numerous existing products continue to lack quality security: one survey indicated almost 65 percent of healthcare IoT products relay sensitive information via insufficient encryption, and 72 percent of them do not implement appropriate access control. This points out a compliance gap as a result of technical and economic limitations.

There are other challenges in key management and user experience. The process of distributing and storing the cryptographic keys on small devices (and updating or revoking them when necessary) is not that easy. In case the security measures are too inquisitive (e.g., need frequent re-authentication of the user or complex configuration), the user can disable them or manufacturers can find workarounds, compromising compliance.

Also, the medical IoT ecosystem may have legacy devices (such as older glucose monitors or cardiac implants) which do not support newer encryption algorithms or remote update mechanisms, and are a weak point.

Emerging Solutions and Best Practice: To address these issues with compliance requirements, researchers and industry are considering new methods. The first option is the lightweight cryptography, i.e., algorithms designed to run on constraint devices. Lightweight ciphers (including PRESENT, XTEA and the recently standardized ASCON family) are created to consume less memory and less power yet offer high encryption strength [54]. Indeed, in 2023, NIST came to the end of a competition spanning many years by choosing Ascon as a new lightweight cryptography standard, namely to protect IoT devices with the smallest overhead [57].

Studies have compared many such ciphers for healthcare IoT: for example, one 2024 experiment evaluated 8 lightweight algorithms on a microcontroller and identified RECTANGLE (a bit-sliced block cipher) as the most efficient for wearable health data, due to its speed and low energy consumption [58]. Implementing these algorithms can help wearables meet encryption requirements without quickly draining their batteries. complex cryptography operation or data processing can be performed on nearby hubs (which is more powerful) by an edge computing architecture, allowing the wearable device itself to be light. This idea also makes it possible to do federated learning and on-device data processing to improve privacy: instead of uploading raw personal information to the cloud, a wearable can locally encrypt or summarize the data, upload only insights that are necessary, or engage in federated machine learning where only model updates (not identifiable data) are transmitted [26]. Physically unclonable functions (PUFs) are becoming popular in terms of authentication to achieve device identity with low overhead. Scholars have also proven PUF-based mutual authentication protocols of wearables that offer high security at low cost. Yu and Park [31] demonstrated a PUF-enabled group authentication scheme that was able to authenticate multiple wearable sensors at once and was more efficient than the traditional digital key storage. Such PUF-enabled authentication techniques can be used to solve major management problems and can even enable the use of zero-power authentication (by taking advantage of the physics of the device itself instead of the additional CPU cycles). Homomorphic encryption (HE) allows calculations to be performed on encrypted information; say a cloud service could perform analytics on encrypted glucose measurements of a wearer and provide results without ever decrypting the underlying data. This may become a compliance game changer, since it ensures that personal data is encrypted throughout [59]. Older fully homomorphic encryption was too slow to be practicable in wearables, but more recent schemes and hybrid designs are being developed. A recent application involved an aggregation of health data on wearables with a lightweight lattice-based HE, which was able to run a secure computation with 40 percent less energy than conventional algorithms. Despite being a relatively new technology, customized HE or partial homomorphic algorithms (e.g., simple averages or trend computations under encryption) may soon enable cloud computing of wearable data without revealing individuals, hence addressing very stringent privacy concerns. Other than cryptography, there is a trend towards end-to-end medical IoT security. This involves the use of such measures as secure boot (no unauthorized firmware on the devices), frequent over-the-air updates on security patches, intrusion detection system on abnormal device behavior and a more stringent validation in the app stores on companion apps. The interoperability vs. security dilemma can be mitigated by adopting open interoperability standards that incorporate security (e.g., the IEEE 11073 health device standards with encryption, or HL7 FHIR with access controls) - all ecosystem participants would be using a standard security protocol. Regulators and industry groups have also begun developing certification schemes for cybersecurity in medical devices (for instance, the EU MDR's guidance MDCG 2019-16 and the US FDA's premarket cybersecurity draft guidance), which encourage use of these best practices and "state of the art" encryption. Going forward, experts advocate for even more advanced strategies like post-quantum cryptography to future-proof wearables. While quantum-resistant algorithms (lattice-based, hash-based, etc.) are not yet commonly implemented in wearables, planning for them is wise given device lifespans. A 2024 roadmap on post-quantum healthcare security emphasizes timely adoption of quantum-safe encryption in health IoT systems to ensure resilience against future threats [42]. This has indicated that compliance goes beyond regulatory concerns and needs to be considered in the design of the devices, secure data flows, effective encryption schemes and consent mechanisms that place the user at the center.

## 9. CASE STUDIES OF COMPLIANCE FAILURES IN WEARABLE/MEDICAL IOT DEVICES

The publicity of the security breaches in wearable and medical IoT devices highlights the extreme repercussions of insufficient encryption, weak authentication, or the lack of data control. Over the recent years, there have been multiple instances in which lack of device security or privacy measures resulted in regulatory measures, patient safety, or even

controversy among the population. We cover a set of real-world events (between fitness trackers and life and death medical implants) that demonstrate how lack of compliance may lead to breaches, recalls, and legal fines.

Insulin Pump Recalls and Vulnerabilities: In June 2019, an insulin pump recall was voluntary, as the FDA announced it would recall some Medtronic insulin pumps because of cybersecurity risks - the first security-related device recall of diabetes equipment [32]. These were the early IoT medical devices, insulin pumps that were wirelessly connected to controllers and did not have sufficient encryption or access controls. Security researchers discovered that an attacker at radio range could pick up transmissions and might alter the dosage commands of the pump. Practically, the pump can be hacked to administer harmful doses of insulin without the user noticing it, and this is done wirelessly. This extreme weakness was due to the fact that the pump was based on an insecure communication protocol (no modern encryption, and authentication that could be compromised easily). It was evident that the compliance failure occurred: the device was not the state of the art security needed to secure patients. The outcome was a Class I recall (the most serious type) and a safety warning that tens of thousands of patients should switch to newer and safer models. Medtronic offered free upgrades to enhanced encryption and turned off the dangerous remote dosing functionality [60]. Although there were no previously known instances of patient harm prior to the fix, the accident made FDA and regulators tighten the requirements - it proved that loose security of an IoT-based medical device could directly cause loss of lives, which is an unacceptable risk according to regulations. It was also the first of its kind: manufacturers got put on toes to understand that cybersecurity negligence might result in expensive recalls and responsibility. In fact, after this case, FDA hastened the publication of official cybersecurity regulations of medical devices.

Hacks and Patches of Cardiac Devices: The case with the insulin pump was not an isolated one. About the same period, scientists revealed grave defects in implantable cardiac devices (such as pacemakers and defibrillators) manufactured by St. Jude Medical (since acquired by Abbott) [55, 61]. In 2017, the FDA issued a safety alert and the manufacturer released a patch to the firmware of the pacemakers to mandate encryption of transmissions and authentication handshakes (approximately 500,000 pacemakers). That may be discussed as a so-called stealth recall - patients were forced to visit clinics to update their device because there was a compliance issue with the initially designed one. The vulnerabilities should an attacker exploit them, they may drain the device battery or alter pacing commands and this may affect the device negatively. Regulatively, the lack of encryption/authentication contravened the need to provide device safety and effectiveness (since explicitly highlighted by MDR and FDA guidance's). The resultant effects were not limited to the release of patches but also the tarnished reputation and litigation. Such incidents made healthcare providers seek cybersecurity evidence by manufacturers. In a review, researchers have observed that current FDA policies establish a set of good practices but are not enforceable. The size of devices also constrains asymmetric cryptography, which is regrettable because such design justifications did not stop attacks in the real world. The lesson was that manufacturers could be sued in regard to retrofitting security or withdrawal of products. In 2021 the regulators themselves recalled even some new Class I models of pacemakers (in those cases due to battery defects) [61, 62], and this shows that any perceived threat will lead to a stern corrective response. The vulnerabilities of pacemakers also led to more general industry reform: subsequent models across competitors started to include encryption, and the US Congress has amended the medical device legislation (in the 2022 amendments of the FD&C Act) to make it mandatory that cybersecurity plans be included in pre-market submissions [53].

Fitness Tracker Data Breach (MyFitnessPal App): Not every breach of compliance requires a hoodie hacker, as in some cases, the data leak is caused by insufficient internal controls or management. One of the best examples is the MyFitnessPal breach of 2018, which is one of the largest containing wearable/fitness data. MyFitnessPal (a fitness app and wearable platform owned by Under Armour) was attacked and the personal information of 150 million users was disclosed, including credentials to access the application and potentially health profile data. Data was not encrypted in rest (hashed passwords but plaintext other data was used), and the attack was explained by the inability of unauthorized access to systems of the company. Despite the fact that this event occurred before 2021, it is often used in recent literature as a warning example [63]. It also underscored the potential of a huge breach of privacy due to data governance being misaligned (poor database security, absence of encryption of sensitive data, etc.). After this, several class-action suits were initiated and the company suffered a tarnished image. The case also demonstrated cross-jurisdictional regulatory impact: EU authorities examined whether GDPR applied (it happened just before GDPR enforcement) and U.S. regulators noted that failure to protect user data could violate consumer protection laws. In current discussions, scholars assert that such breaches show the need for stronger encryption of wearable cloud databases and better access control. The average cost of a health data breach has risen to over $4 million, and MyFitnessPal's incident likely contributed to that statistic. Importantly, this case spurred many fitness and mHealth companies to reevaluate their compliance: data that was previously stored in identifiable form is now increasingly encrypted or tokenized in databases, and companies are more transparent with users about data practices.

Strava Heatmap and Geolocation Privacy: In early 2018, a social fitness platform Strava inadvertently revealed sensitive information through its publicly available activity heatmaps. Strava aggregated GPS tracks from millions of users' wearable fitness devices (running/cycling routes) and published a global "heatmap." Investigative users discovered that the map could pinpoint the internal routes of soldiers on military bases (who were using fitness trackers), effectively mapping out classified locations. Although Strava had technically anonymized the data, it was not truly de-identified – rare or sensitive patterns (like jogging laps inside a forward operating base) were easily re-identified [33]. Although it was not a hack or breach, it had severe security repercussions and prompted the military agencies to prohibit wearables in specific areas. Compliance-wise, Strava was questioned on the issue of the possible insufficiency of the anonymization of personal data as required by the GDPR and other laws. It highlighted the fact that it is not just enough to remove names, but location traces may be personal data when people can be re-identified. The company soon added more fine-tuning privacy options (giving users the ability to opt-out of heatmaps altogether) and changed its data sharing policies.

Wearable Data Misuse and Legal Implications: In addition

to breaches and hacks, wearable data has been misused in a number of other ways that do not comply with privacy regulations. An example is employers wearing wellness devices or fitness trackers on employees without having the necessary protection. To illustrate, when an employer requires employees to wear wearables to track their health or productivity, they have to comply with GDPR/EEOC regulations, they were even warned against this by a regulator in 2022 (no fine was imposed, but the policies had to be changed) because the use of fitness trackers was considered excessive and was not in line with data minimization (no formal fine was imposed, but the policies had to change) [64]. Another new problem is law enforcement access to wearable data: in some court cases, litigants have requested wearable data (e.g., heart rate, number of steps) to support or refute claims about an incident. In a 2021 U.S. case, a prosecutor relied on Fitbit data to prove a timeline of the death of a victim, which cast doubt on the issue of consent and proper subpoena procedure of such data.

General Increase in Health IoT Breaches: The trend is worrying, besides isolated cases. Cyberattacks have gained popularity in the area of healthcare IoT devices and wearables. In 2021, 45 million health data of individuals were affected by breaches, which significantly increased compared to 34 million the previous year [65]. A lot of these accidents can be traced to stolen or unsecured wearable/IoMT data - such as unsecured cloud services to store fitness apps, or third-party health IoT integrations. This kind of violation usually leads to inquiries and fines. In the US, under HIPAA, a number of digital health companies have been fined over the past few years following breaches, particularly when it is established that the data was not adequately encrypted, or when there was a delay in the reaction to the incident. The wearable data silos have become the target of attacks (ransomware, API hacks, etc.), which has compelled companies to enhance compliance efforts post-factum. According to one report, more than 50 percent of IoMT devices are estimated to be susceptible to attack, and the list of reported attacks against wearables is growing annually. This has raised the eyebrows of regulators across the world. As an example, in 2022, the European Data Protection Board organised a coordinated enforcement operation on health wearables, which investigated whether companies provide sufficient information to users and protect the massive personal data gathered by these devices. Compliance is being fuelled by the implicit threat of fines and bans: firms which experienced breaches have been forced to put in place detailed corrective action plans under the supervision of regulators, which may include encryption of all personal data, strong authentication of systems and periodic security audits [66].

All these examples (including life-saving medical devices and consumer fitness apps) support a similar point: failure to comply with security and privacy standards in wearable technology may have disastrous effects.

Although there is a certain overlap of legal, technical, and ethical fields, this is the nature of the compliance issues in wearable IoT systems, which are interconnected.

## 10. CONCLUSION

The review examined the issues of adhering to the regulations of wearing IoT devices that control health through the prism of legal, technical, and ethical aspects in a structured manner. The paper underlines that, although significant progress has been made in legal frameworks and security procedures, compliance in wearable systems remains uncoordinated due to differences in jurisdiction and types of devices and the level of sensitivity of the data. Among the essential facts that the review discovered is that compliance cannot be a distinct legislative requirement. Rather, it must be designed directly into the system architecture based on privacy-by-design, secure data architecture, and consent-based processes that are user-friendly. It has been analyzed that gaps in the literature remain, including the absence of global standards to collaborate, the scarcity of lightweight security solutions to work with wearables, lacking a substantial amount of resources, and the lack of emphasis on fairness, transparency, and user trust in health apps utilizing data. There is also the disparity between the top-level regulatory mandates and their actual implementation in device-level architectures, as a significant issue. Filling in these gaps, future studies must address the need to create compliance frameworks that work hand in hand, enhance security solutions capable of evolving and expanding, and also account for ethical issues in the design and use of wearable IoT devices. The survey is a systematic review of prior studies and some recommendations, which can be implemented to enhance the creation of compliant, secure, and reliable wearable health solutions.

## REFERENCES


[1] Chandrasekaran, R., Sadiq, T.M., Moustakas, E. (2025). Usage trends and data sharing practices of healthcare wearable devices among US adults: Cross-sectional study. Journal of Medical Internet Research, 27: e63879. https://doi.org/10.2196/63879

[2] Powell, D., Godfrey, A. (2023). Considerations for integrating wearables into the everyday healthcare practice. NPJ Digital Medicine, 6(1): 70. https://doi.org/10.1038/s41746-023-00820-z

[3] Hughes-Lartey, K., Li, M., Botchey, F.E., Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7(3): e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

[4] Smith, A.A., Li, R., Tse, Z.T.H. (2023). Reshaping healthcare with wearable biosensors. Scientific Reports, 13(1): 4998. https://doi.org/10.1038/s41598-022-26951-z

[5] 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(10): e0000104. https://doi.org/10.1371/journal.pdig.0000104

[6] Ioannidou, I., Sklavos, N. (2021). On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. Cryptography, 5(4): 29. https://doi.org/10.3390/cryptography5040029

[7] Özçağdavul, M. (2024). General data protection regulation compliance and privacy protection in wearable health devices: Challenges and solutions. Artuklu Health, 10: 29-37. https://doi.org/10.58252/artukluhealth.1566573

[8] Sifaoui, A., Eastin, M.S. (2024). “Whispers from the

wrist": Wearable health monitoring devices and privacy regulations in the US: The loopholes, the challenges, and the opportunities. Cryptography, 8(2): 26. https://doi.org/10.3390/cryptography8020026

[9] Iqbal, J.D., Biller-Andorno, N. (2022). The regulatory gap in digital health and alternative pathways to bridge it. Health Policy and Technology, 11(3): 100663. https://doi.org/10.1016/j.hlpt.2022.100663

[10] Barua, A., Al Alamin, M.A., Hossain, M.S., Hossain, E. (2022). Security and privacy threats for bluetooth low energy in IoT and wearable devices: A comprehensive survey. IEEE Open Journal of the Communications Society, 3: 251-281. https://doi.org/10.1109/OJCOMS.2022.3149732

[11] Espinoza, J., Xu, N.Y., Nguyen, K.T., Klonoff, D.C. (2023). The need for data standards and implementation policies to integrate CGM data into the electronic health record. Journal of Diabetes Science and Technology, 17(2): 495-502. https://doi.org/10.1177/19322968211058148

[12] Sui, A., Sui, W., Liu, S., Rhodes, R. (2023). Ethical considerations for the use of consumer wearables in health research. Digital Health, 9: 20552076231153740. https://doi.org/10.1177/20552076231153740

[13] Colvonen, P.J., DeYoung, P.N., Bosompra, N.O.A., Owens, R.L. (2020). Limiting racial disparities and bias for wearable devices in health science research. Sleep, 43(10): zsaa159. https://doi.org/10.1093/sleep/zsaa159

[14] Brannon, G.E., Mitchell, S., Liao, Y. (2022). Addressing privacy concerns for mobile and wearable devices sensors: Small-group interviews with healthy adults and cancer survivors. PEC Innovation, 1: 100022. https://doi.org/10.1016/j.pecinn.2022.100022

[15] Taka, A.M. (2023). A deep dive into dynamic data flows, wearable devices, and the concept of health data. International Data Privacy Law, 13(2): 124-140. https://doi.org/10.1093/idpl/ipad007

[16] Tziouras, J. (2022). Health data from wearable technologies: Privacy and security regulatory aspects. Master Thesis.

[17] Sai, K.J. (2024). Digital data protection act, 2023. International Journal of Law Management & Humanities, 7: 1053.

[18] Colloud, S., Metcalfe, T., Askin, S., Belachew, S., Ammann, J., Bos, E., Kilchenmann, T., Strijbos, P., Eggenspieler, D., Servais, L., Garay, C., Konstantakopoulos, A., Ritzhaupt, A., Vetter, T., Vincenzi, C., Cerreta, F. (2023). Evolving regulatory perspectives on digital health technologies for medicinal product development. NPJ Digital Medicine, 6(1): 56. https://doi.org/10.1038/s41746-023-00790-2

[19] Malvehy, J., Ginsberg, R., Sampietro-Colom, L., Ficapal, J., Combalia, M., Svedenhag, P. (2022). New regulation of medical devices in the EU: Impact in dermatology. Journal of the European Academy of Dermatology and Venereology, 36(3): 360-364. https://doi.org/10.1111/jdv.17830

[20] Ash, G.I., Stults-Kolehmainen, M., Busa, M.A., et al. (2021). Establishing a global standard for wearable devices in sport and exercise medicine: Perspectives from academic and industry stakeholders. Sports Medicine, 51(11): 2237-2250. https://doi.org/10.1007/s40279-021-01543-5

[21] Guidance, W.H.O. (2021). Ethics and governance of artificial intelligence for health. World Health Organization, 1-165.

[22] Devine, J.K., Schwartz, L.P., Hursh, S.R. (2022). Technical, regulatory, economic, and trust issues preventing successful integration of sensors into the mainstream consumer wearables market. Sensors, 22(7): 2731. https://doi.org/10.3390/s22072731

[23] Khan, F., Kim, J.H., Mathiassen, L., Moore, R. (2021). Data breach management: An integrated risk model. Information & Management, 58(1): 103392. https://doi.org/10.1016/j.im.2020.103392

[24] Bouderhem, R. (2023). Privacy and regulatory issues in wearable health technology. Engineering Proceedings, 58(1): 87. https://doi.org/10.3390/ecsa-10-16206

[25] Act, A.I. (2021). Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. EUR-Lex-52021PC0206.

[26] Said, A., Yahyaoui, A., Abdellatif, T. (2023). HIPAA and GDPR compliance in IoT healthcare systems. In Advances in Model and Data Engineering in the Digitalization Era, pp. 198-209. https://doi.org/10.1007/978-3-031-55729-3_16

[27] Brönneke, J.B., Müller, J., Mouratis, K., Hagen, J., Stern, A.D. (2021). Regulatory, legal, and market aspects of smart wearables for cardiac monitoring. Sensors, 21(14): 4937. https://doi.org/10.3390/s21144937

[28] Thakor, V.A., Razzaque, M.A., Khandaker, M.R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9: 28177-28193. https://doi.org/10.1109/ACCESS.2021.3052867

[29] Zhou, H. (2023). Comparison of encryption algorithms for wearable devices in IoT systems. Engineering Advances, 3(2): 144-148. http://doi.org/10.26855/ea.2023.04.013

[30] Chinbat, T., Madanian, S., Airehrour, D., Hassandoust, F. (2024). Machine learning cryptography methods for IoT in healthcare. BMC Medical Informatics and Decision Making, 24(1): 153. https://doi.org/10.1186/s12911-024-02548-6

[31] Yu, S., Park, Y. (2023). Robust and efficient authentication and group–proof scheme using physical unclonable functions for wearable computing. Sensors, 23(12): 5747. https://doi.org/10.3390/s23125747

[32] Klonoff, D., Han, J. (2019). The first recall of a diabetes device because of cybersecurity risks. Journal of Diabetes Science and Technology, 13(5): 817-820. https://doi.org/10.1177/1932296819865655

[33] Alam, M.A.U. (2021). Person re-identification attack on wearable sensing. arXiv preprint arXiv:2106.11900. https://doi.org/10.48550/arXiv.2106.11900

[34] Aminifar, A., Shokri, M., Aminifar, A. (2024). Privacy-preserving edge federated learning for intelligent mobile-health systems. Future Generation Computer Systems, 161: 625-637. https://doi.org/10.1016/j.future.2024.07.035

[35] Ghadi, Y.Y., Mazhar, T., Shahzad, T., Amir Khan, M., Abd-Alrazaq, A., Ahmed, A., Hamam, H. (2024). The role of blockchain to secure internet of medical things. Scientific Reports, 14(1): 18422. https://doi.org/10.1038/s41598-024-68529-x

[36] Shahid, J., Ahmad, R., Kiani, A.K., Ahmad, T., Saeed, S.,

Almuhaideb, A.M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, 12(4): 1927. https://doi.org/10.3390/app12041927

[37] Dobson, R., Stowell, M., Warren, J., Tane, T., Ni, L., Gu, Y., McCool, J., Whittaker, R. (2023). Use of consumer wearables in health research: Issues and considerations. Journal of Medical Internet Research, 25: e52444. https://doi.org/10.2196/52444

[38] Azodo, I., Williams, R., Sheikh, A., Cresswell, K. (2020). Opportunities and challenges surrounding the use of data from wearable sensor devices in health care: Qualitative interview study. Journal of Medical Internet Research, 22(10): e19542. https://doi.org/10.2196/19542

[39] Chikwetu, L., Miao, Y., Woldetensae, M.K., Bell, D., Goldenholz, D.M., Dunn, J. (2023). Does deidentification of data from wearable devices give us a false sense of security? A systematic review. The Lancet Digital Health, 5(4): e239-e247. https://doi.org/10.1016/S2589-7500(22)00234-5

[40] Garg, M. (2025). Adaptive differential privacy in federated edge AI for medical IoT: Energy-efficient, HIPAA-compliant frameworks for distributed real-time diagnostics. Journal of Information Systems Engineering and Management, 10(34): 36-44. https://doi.org/10.52783/jisem.v10i34s.5773

[41] Asif, M., Abrar, M., Salam, A., Amin, F., Ullah, F., Shah, S., AlSalman, H. (2025). Intelligent two-phase dual authentication framework for Internet of Medical Things. Scientific Reports, 15(1): 1760. https://doi.org/10.1038/s41598-024-84713-5

[42] SaberiKamarposhti, M., Ng, K.W., Chua, F.F., Abdullah, J., Yadollahi, M., Moradi, M., Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon, 10(10): e31406. https://doi.org/10.1016/j.heliyon.2024.e31406

[43] Hamed, S.B., Hamed, M.B., Sbita, L., Bajaj, M., Blazek, V., Prokop, L., Misak, S., Ghoneim, S.S. (2022). Robust optimization and power management of a triple junction photovoltaic electric vehicle with battery storage. Sensors, 22(16): 6123. https://doi.org/10.3390/s22166123

[44] Torre, I., Koceva, F., Sanchez, O.R., Adorni, G. (2016). A framework for personal data protection in the IoT. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, pp. 384-391. https://doi.org/10.1109/ICITST.2016.7856735

[45] Winter, J.S., Davidson, E. (2022). Harmonizing regulatory regimes for the governance of patient-generated health data. Telecommunications Policy, 46(5): 102285. https://doi.org/10.1016/j.telpol.2021.102285

[46] Chapman, B.P., Lucey, E., Boyer, E.W., Babu, K.M., Smelson, D., Carreiro, S. (2022). Perceptions on wearable sensor-based interventions for monitoring of opioid therapy: A qualitative study. Frontiers in Digital Health, 4: 969642. https://doi.org/10.3389/fdgth.2022.969642

[47] Azodo, I., Williams, R., Sheikh, A., Cresswell, K. (2020). Opportunities and challenges surrounding the use of data from wearable sensor devices in health care: Qualitative interview study. Journal of Medical Internet Research, 22(10): e19542. https://doi.org/10.2196/19542

[48] O'Neill, E. (2022). Contextual Integrity as a General Conceptual Tool for Evaluating Technological Change. Philosophy & Technology, 35(3): 79. https://doi.org/10.1007/s13347-022-00574-8

[49] Chikwetu, L., Miao, Y., Woldetensae, M.K., Bell, D., Goldenholz, D.M., Dunn, J. (2023). Does deidentification of data from wearable devices give us a false sense of security? A systematic review. The Lancet Digital Health, 5(4): e239-e247. https://doi.org/10.1016/S2589-7500(22)00234-5

[50] Xiang, D., Cai, W. (2021). Privacy protection and secondary use of health data: Strategies and methods. BioMed Research International, 2021(1): 6967166. https://doi.org/10.1155/2021/6967166

[51] Hydari, M.Z., Adjerid, I., Striegel, A.D. (2023). Health wearables, gamification, and healthful activity. Management science, 69(7): 3920-3938. https://doi.org/10.1287/mnsc.2022.4581

[52] Lin, Y., Juneja, J., Birrell, E., Cranor, L.F. (2023). Data safety vs. app privacy: Comparing the usability of android and IOS privacy labels. arXiv preprint arXiv:2312.03918. https://doi.org/10.48550/arXiv.2312.03918

[53] Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., Gilbert, S. (2024). Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: Scoping review. Journal of Medical Internet Research, 26: e65528. https://doi.org/10.2196/65528

[54] Thakor, V.A., Razzaque, M.A., Khandaker, M.R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9: 28177-28193. https://doi.org/10.1109/ACCESS.2021.3052867

[55] Das, S., Siroky, G.P., Lee, S., Mehta, D., Suri, R. (2021). Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. Heart Rhythm, 18(3): 473-481. https://doi.org/10.1016/j.hrthm.2020.10.009

[56] Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A., Yelamarthi, K. (2022). Prospect of internet of medical things: A review on security requirements and solutions. Sensors, 22(15): 5517. https://doi.org/10.3390/s22155517

[57] NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices. (2023). https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices.

[58] Chinbat, T., Madanian, S., Airehrour, D., Hassandoust, F. (2024). Machine learning cryptography methods for IoT in healthcare. BMC Medical Informatics and Decision Making, 24(1): 153.

[59] Shin, H., Ryu, K., Kim, J.Y., Lee, S. (2024). Application of privacy protection technology to healthcare big data. Digital Health, 10: 20552076241282242. https://doi.org/10.1177/20552076241282242

[60] Al-Allawee, A., Lorenz, P., Munther, A. (2024). Efficient collaborative edge computing for vehicular network using clustering service. Network, 4(3): 390-403. https://doi.org/10.3390/network4030018

[61] Kuehn, B.M. (2018). Pacemaker Recall Highlights Security Concerns for Implantable Devices. Lippincott Williams & Wilkins Hagerstown, MD. https://doi.org/10.1161/CIRCULATIONAHA.118.037331

[62] El-Chami, M.F. (2021). Cardiac implantable device recalls: Consequences, and management. HeartRhythm Case Reports, 7(12): 795-796. https://doi.org/10.1016/j.hrcr.2021.11.005
[63] IoT Security: Are IoT Wearable Devices a Cybersecurity Risk? https://www.triaxtec.com/blog/iot-security-are-iot-wearable-devices-a-cybersecurity-risk/#:~:text=The%20cost%20of%20a%20data,questions%20around%20security%20risks.
[64] Ajunwa, I. (2018). Algorithms at work: Productivity monitoring applications and wearable technology as the new data-centric research agenda for employment and labor law. Louis ULJ, 63(1): 21.
[65] Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A. (2022). Internet of things: Security and solutions survey. Sensors, 22(19): 7433. https://doi.org/10.3390/s22197433
[66] Khan, N.E., Rudman, R.J. (2025). IoT medical device risks: Data security, privacy, confidentiality and compliance with HIPAA and COBIT 2019. South African Journal of Business Management, 56(1): 4796. https://hdl.handle.net/10520/ejc-busman_v56_n1_a4796.