“Whispers from the Wrist”: Wearable Health Monitoring Devices and Privacy Regulations in the U.S.: The Loopholes, the Challenges, and the Opportunities

Asma Sifaoui * and Matthew S. Eastin

Stan Richards School of Advertising and Public Relations, Moody College of Communication, The University of Texas at Austin, Austin, TX 78712, USA; matt.eastin@utexas.edu
* Correspondence: asma.sifaoui@utexas.edu

Abstract: The growth of wearable technology has enabled the collection of even more personalized information on individuals. New health-related devices marketed to consumers collect health information that might not fall under the traditional category of Protected Health Information, and thus, HIPAA protections do not fully apply. Meaning, commercial wearable health devices do not fall under FDA oversight, and data not paired with a doctor–patient relationship do not fall under HIPAA privacy protection; thus, much of the gathered health-related metrics are left without regulation and open to be sold to data brokers. As such, these data can be leveraged by health insurance, law enforcement, and employers, to name a few. This manuscript explores the loopholes in current regulations and suggests a framework that categorizes wearable data and addresses challenges in data transfer. Furthermore, taking a user perspective, the suggested framework offers solutions that aim to guide users and policymakers in navigating privacy issues in wearable technology.

Keywords: wearables; health data; privacy; regulations

1. Introduction

Wearable technology has experienced exponential growth in recent years, with devices like smartwatches and fitness trackers becoming increasingly ubiquitous. These technologies provide unprecedented insights into various personal health metrics, including heart rates, sleep patterns, dietary habits, exercise levels, activity levels, and even stress and mental health data [1]. Access to this wide range of personal information has offered users the ability to track and improve their overall well-being in real-time, which allows users to be more health-conscious [2,3]. Furthermore, wearable technology has opened up new possibilities for healthcare professionals to monitor and manage patient health more efficiently [4,5].

Classified into four categories by Healey, Pollard, and Woods, wearable health devices encompass a spectrum ranging from wearable health monitoring devices to stationary medical devices [6]. This study focuses specifically on wearable health monitoring devices (WHMDs), such as Fitbit and Apple Watch, designed for consumer use. While the distinction between consumer health wearables and medical devices is becoming increasingly blurred, consumer health wearables, or WHMD, have a primary focus on tracking and monitoring personal health and fitness data for individuals [7]. These devices are typically used for wellness purposes rather than medical diagnosis or treatment. However, recent technological advancements are taking what were simple metrics to more advanced health tracking capabilities such as blood glucose levels, oxygen levels, and temperature. Consumer health wearables have the potential to provide individuals with direct access to personal analytics that may help in managing their health and illnesses [8]. However, the digitization of healthcare and well-being, especially through wearable technology, has created new challenges for individuals, healthcare professionals, and regulators.
The extensive amount of data being generated by these wearables present various privacy and security concerns. The data collected can be used for various purposes and by different parties, such as insurance companies and employment determinations, thus posing privacy risks and infringements on individuals’ privacy rights [7]. Furthermore, the abundance of information and its transfer through a network of advertisers and data brokers pose challenges to individuals’ ability to understand consent and the implications of sharing personal data through these new technologies.

In fact, data generated from WHMD intersect the lack of a comprehensive privacy framework in the U.S. and the limitations of existing regulations like the Health Insurance and Portability Accountability Act (HIPAA). While HIPAA provides some protection for health information under the Privacy Rule and the Security Rule, it primarily applies to healthcare providers, insurers, and their business associates, and thus, leaves a significant gap in the protection of consumer-generated health data. This regulatory gap raises concerns regarding the privacy and security of these data. More specifically, what legal protections apply to health data that do not meet the legal definition of Protected Health Information (PHI) as outlined by HIPAA, yet are still shared, utilized, and sold by third parties not subject to HIPAA regulations?

There are many concerns regarding the validity and reliability of the data generated by WHMDs, which lack U.S. Food and Drug Administration (FDA) scrutiny. In fact, many WHMD and health apps are developed by companies not subject to FDA oversight. Indeed, an FDA mandate is only required for medical devices, and thus WHMDs fall outside the scope of regulatory oversight. The lack of standardized regulations concerning consumer health information produced by WHMDs poses challenges to the accuracy of the generated data. This amplifies users’ risks of misinterpretation of their health and potential misuse of personal information by third parties, especially when these intimate data can be bought and sold to data brokers and insurance companies.

Through an examination of current legal frameworks in the U.S., including but not limited to HIPAA, this study seeks to elucidate the gaps and shortcomings in addressing the unique privacy concerns posed by health information generated by these types of wearables. Currently, operating in a regulatory gray area lacking oversight of data brokers, consumer health data generated by wearables raise significant privacy concerns and risks for individuals. The shortcomings of such regulations highlight the need for updated legislation to protect the privacy of individuals using health monitoring devices and fitness trackers. Simply, the current lack of oversight on the device metrics creates an unregulated accuracy issue for users, and the lack of comprehensive privacy regulation opens users to privacy violations through the unregulated dissemination of data. Moreover, as outlined below, it is also important to understand how and with what efficacy consumers interpret and understand digital contracts, as this is the initial barrier to potential privacy violations.

To this end, this current manuscript provides a new framework that categorizes data generated by wearables and looks at the challenges that arise in the transfer of data to different parties. The framework provides solutions and considerations for users and policymakers that aim to navigate the evolving landscape of wearable technology and privacy legislation. In doing so, this research expands upon the existing literature on wearable technology for consumer use and provides practical recommendations for different stakeholders to enhance privacy protection in the use of wearables collecting health information. By addressing these gaps, this study aims to contribute to the ongoing discussion of data privacy in the context of emerging technologies.

2. Wearables and Health Data

The evolution of wearables and the growth of health data have catalyzed a transformative shift in personal healthcare and have ushered in a new era of personal wellness monitoring [5,9,10]. Wearable technology, or simply wearables, ranging from smartwatches to fitness trackers, have been seamlessly integrated into the daily lives of consumers. Through various integrated apps and devices, users are able to track their heart rate, sleep
patterns, activity levels (such as steps), blood glucose levels, oxygen levels, temperatures and can even be used as trackers for mental health levels (such as stress) [1]. Individuals can also enter their calory intake and medications for better personalization. The influx of health capabilities has enabled individuals to take proactive steps towards improving their well-being, as well as revolutionizing the healthcare landscape.

The integration of these devices has significantly influenced the landscape of apps and wearable technology. In fact, following the introduction of smartwatches to the market by major smartphone manufacturers such as Apple and Samsung in 2014, the smartwatch has emerged as the predominant type of wearable technology, constituting 44.2 percent of the overall wearable device market [11]. The smartwatch allows users to track health metrics such as sleep patterns, heart rate, and movement. Recently, research claims that smartwatch monitoring “shows promise in detecting heart diseases, movement disorders, and even early signs of COVID-19” [12] (p. 248). Furthermore, according to a report by Deloitte on U.S. Healthcare & Consumers, there is a rising number of individuals utilizing wearables, applications, digital assistants, and smart devices to monitor their fitness and health improvement goals, with percentages increasing from 42% in 2018 to 49% in 2022. Similarly, the use of these technologies for monitoring health concerns has also seen an uptick, rising from 27% in 2018 to 34% in 2022 [13].

Health apps are also part of a consumer phenomenon that has seen rapid growth in mobile software and hardware. It is estimated that over 300 million individuals used health apps in 2023 [14]. These trends are supported by the Health Information National Trends Survey which reported that almost one in three Americans use a wearable device, such as a smart watch or band, to track their health and fitness. This figure is estimated to continue growing over the next few years [15]. These digital apps offer tools to users to monitor and self-manage their health and well-being, and while these practices are becoming commonplace, the opportunities and challenges of collecting and sharing personal and sensitive information keep growing.

3. The Issues with Wearables and Health Data

3.1. Lack of Regulation over WHMD and Health Apps Marketed for Consumers

Information collected through the integration of wearables and health apps ranges from demographic information, such as age, gender, and location, to more detailed data related to individuals’ health and well-being [5]. Biometric data have become increasingly prevalent, with individuals using fingerprints or facial recognition to unlock wearable devices [16]. This information is collected and then pieced together to create a consumer profile that provides insights into an individual’s preferences, interests, and behaviors.

Data are also transferred to marketers for personalized marketing strategies [17]. Businesses rely on data to make more informed decisions in a world where competition is fierce and customer expectations are constantly evolving. The need for efficiency and effectiveness has allowed businesses such as data brokers to flourish, as they specialize in collecting and analyzing vast amounts of consumer data [18]. These data give marketers access to the minds of consumers, enabling them to understand their needs and desires on an even deeper level [19]. Behind these various interactions lies a lucrative business model for many companies that rely on the commodification and commercialization of individuals’ personal information [18]. Indeed, this exchange often occurs without a full understanding of the implications for individuals’ privacy and autonomy. As wearables become increasingly ubiquitous, tracking our every move, heartbeat, and sleep pattern, the stakes of this tradeoff rise even higher. While these devices offer valuable insights into health and behavior of individuals, they also raise concerns about data privacy and surveillance.

First, it is important to highlight that WHMDs marketed as a health app generally do not need to have obtained FDA approval, as they do not always fall under the category of medical devices. However, certain WHMDs and health apps are actively pursuing FDA approval, particularly those with capabilities similar to traditional medical devices that require regulatory oversight such as electrocardiography (ECG) technology. An example
of this trend is Fitbit, a manufacturer of wearable fitness trackers [20]. Fitbit has sought FDA approval for certain features and functionalities that elevate its devices beyond a mere consumer gadget to more closely resemble a medical device in terms of functionality and potential impact on users’ health [20]. However, since most of WHMDs and health apps are not FDA-vetted, the reliability of health data generated by wearable devices is questioned, raising accuracy concerns [21].

While tech companies are making efforts to improve accuracy, data from these devices may still have some challenges regarding reliability as it is geared towards consumer use rather than medical use. The American Medical Association (AMA) as well as the FDA caution healthcare professionals and consumers against relying solely on these data for diagnosis. For example, the FDA has been cautioning against the use of smartwatches and smart rings to measure blood glucose levels, as they may not be as accurate as traditional medical devices [22]. The American Medical Association has also been sharing guidelines with healthcare professionals regarding WHMD. In a statement by the association, they emphasized the importance of caution when recommending devices that are not approved or vetted to patients. The association also encouraged healthcare professionals to regularly be updated on the latest research and advancements in WHMD technology to ensure they are providing the best care for their patients [23].

Traditional monitoring devices are often relied upon in clinical research to address health issues such as inactive lifestyles and obesity [8]. However, consumer-marketed wearable health monitoring devices have not been thoroughly studied. That said, research examining the accuracy of health data has mixed results, with some research suggesting relatively accurate measurement [24], while others found the metrics to be somewhat lacking [25]. In other words, the lack of standardization in data collection and analysis methods leads to inconsistencies in the data reported by different devices. The repercussions of such inconsistencies because of a lack of regulatory oversight extend beyond health monitoring to dissemination of misleading information about individuals’ health status or behaviors. Inaccurate and unreliable data generated by WHMDs may be used by various third parties, including insurance companies, employers, and marketers, to make decisions. Health apps and wearables designed for consumer use are not scrutinized to the same extent as medical devices subject to regulatory oversight. Furthermore, privacy and security challenges should be communicated to patients, as these devices present potential risks in terms of data protection and confidentiality.

Currently, the unregulated nature of WHMDs marketed for consumers underscores existing loopholes in health data regulations. This lack of oversight and accountability of WHMDs and health apps create a gap where a category of sensitive health data operates without adequate supervision, thus potentially compromising data integrity and privacy.

3.2. Privacy Regulations Governing Health Information in the U.S.

3.2.1. HIPAA

In the context of wearables, information gathered from healthcare wearables is subject to a range of legal safeguards. Specific laws apply to different sectors, including the Americans with Disabilities Act (ADA), the Children’s Online Privacy Protection Act (COPPA), and the Fair Credit Reporting Act (FCRA). When it comes to personal health information, the main law that protects health information is the Health Information Portability and Accountability Act, or simply HIPAA. In the United States, the primary federal regulation for personal health data is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. This rule was the first to establish a set of national standards for safeguarding individually identifiable health information, known as personal health information (PHI) [26]. HIPAA primarily addresses practices related to individual consent, retention, security, and the transfer of PHI. PHI is legally defined as “any information about health status, provision of health care, or payment for health care that is created or collected by a covered entity (primarily health care providers and health plans) that can be linked to a specific individual” [26]. HIPAA and its regulations require subjects (healthcare providers,
health plans, etc.) and their partners (associates) to comply with multiple data privacy and security requirements. In essence, HIPAA prohibits the subjects stated above from sharing any personal and identifiable health information of a patient with third parties without the patient’s consent [27]. However, the Privacy Rule includes many exceptions to this general rule on sharing a patient’s information; law enforcement is an exception. In cases, where there is a warrant or a subpoena, healthcare providers, for example, may disclose the health data of their patients. While these exceptions might pose some limitations on a person’s privacy rights, HIPAA does offer protection regarding a person’s health records.

The HIPAA “Security Rule” of 1996 mandates that entities accessing PHI must “ensure the confidentiality, integrity, and availability” of this health information. Additionally, these entities are required to notify affected individuals “without unreasonable delay” in the event of a personal data breach.

A primary imitation of HIPAA is that it does not provide those protections when a patient uses digital tools to record, save, disclose, monitor, or manage their health information. In fact, most of the digital apps used for health are not considered medical devices and thus do not require FDA approval [28]. The data being shared with and collected by these apps are managed by the software vendors and are not accessible by healthcare providers, and thus fall outside the HIPAA regulations [29]. More specifically, when a doctor forwards a patient’s health data to either the patient or a third-party app designated by the patient, and subsequently the patient or the app misuses or experiences a breach of the data, the doctor’s health system is not held accountable under HIPAA. Instead, the responsibility falls upon the patient or the third party.

While some patients/users might assume that health and well-being apps are protected by HIPAA since the disclosed data are health sensitive, in reality these digital apps are not considered covered entities according to HIPAA [30]. Moreover, many users are not aware that data that are being collected from apps are generally sent to the vendor and other third parties for analytics and advertising services. Simply, if an individual uses a wearable device to gather health data for personal use, HIPAA regulations do not apply. That said, when a healthcare provider requests a patient to share health data collected through wearable technology, adherence to HIPAA regulations becomes relevant. HIPAA compliance becomes a consideration when wearable devices are connected to a healthcare provider’s electronic health record (EHR) system, which requires compliance. However, if the entity collecting the data is not subject to HIPAA regulations because it is not a covered entity, and the data are generated solely for consumer use rather than directed medical purposes, issues arise [31]. These data can be shared with third parties who are not subject to HIPAA regulations [31].

3.2.2. HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009. HITECH aims to promote the adoption and meaningful use of health information technology, especially electronic health records (EHRs) [32]. HITECH sought to enhance the efficiency, quality, and coordination of patient care. In addition to promoting technology adoption, HITECH strengthened the privacy and security measures established by the Health Insurance Portability and Accountability Act (HIPAA), aiming to better protect patient health information in an increasingly digital world [32]. However, despite these efforts, HITECH has not fully solved the ongoing issues with the privacy and security of consumer health data. While the act has helped in reinforcing the regulatory framework related to ePHI, it has not completely eliminated the risks of unauthorized access, data breaches, and cyber threats when it comes to consumer health data collected through health apps and other wearable technologies.

3.3. Consumer Literacy and Efficacy of Digital Contracts

In the U.S., the regulation of personal information is fragmented; it is sectoral and varies greatly depending on the industry. The lack of a comprehensive federal framework
that regulates personal information leaves consumers vulnerable to inconsistent protection and enforcement measures [33]. Privacy self-management also plays a role in this fragmented landscape, as individuals are often tasked with navigating complex privacy policies and settings on their own. While the framework of notice and consent is commonly used and is intended to give individuals control over their personal information, it can be overwhelming and ineffective due to structural and cognitive problems [33]. Many scholars argue that these problems reside in the structural of the data ecosystem [33–36].

The sheer volume of information and the complexity of privacy settings can result in a lack of meaningful consent, as individuals may not fully understand the implications of their choices [37]. Indeed, many of these terms and conditions are presented in ways that make it harder for consumers to be fully aware of the extent to which their data are being collected, used, and shared [33–35]. The design of these notices further hinders consumers’ ability to make informed decisions about their privacy. Simply, users lacking an awareness and understanding of privacy policies, legal jargon, and data practices further complicates the decision-making process. In fact, individuals have flawed, woeful and incorrect ideas about how and when their privacy is protected [38,39]. Specifically, research indicates that individuals typically lack an awareness and understanding of which personal data are being collected, who is collecting them, and how they are being shared and used [38–40].

Recently, there has been growing attention on the complexities of obtaining and understanding consent on digital platforms from academics, privacy advocates, and regulatory bodies. The digitalization of activities and the need for connectivity has forced individuals to subscribe to an ecosystem that relies on giving consent in exchange of services and activities. Users find themselves bearing the responsibility of the notice and choice framework that places the burden on them to navigate through complex privacy policies and terms of service [41]. In the U.S., organizations rely on the “notice and choice” framework to legitimize the collection, utilization, and processing of data [42]. This framework gives notice to individuals, usually through a privacy notice or terms and conditions, and provides individuals with the right to “accept” or “decline” [42]. Yet, in reality, this approach gives no real choice for individuals since using the services requires them to accept the terms. On the other hand, past research has often looked at this exchange (i.e., access to data) as a privacy paradox where individuals still engage with these organizations while feeling concerned about their interactions and personal data [43]. It is important to highlight that individuals’ expectations of these organizations typically relate to the organization they are interacting with and not the third parties, software developers, partners, etc., who purchase the data. The diffusion of information across different parties exacerbates privacy risks, as individuals’ data can be accessed, used, and shared beyond their initial understanding or consent [41].

The increased complexity surrounding regulations that govern how organizations manage personal information based on their specific contexts could lead to varied expectations among consumers regarding their data. In the context of health data from WHMDs, the differing regulations for Protected Health Information (PHI) versus other personal health information make it hard for consumers to know which rules apply to their data. In fact, a recent study showed that 82% of Americans do not know that HIPAA does not prevent apps from selling data collected about users [39].

3.4. Data Brokers and Personal Information

Health data hold significant value to data brokers due to their intimate nature and potential insights into individuals’ health conditions, behaviors, and preferences. In fact, there are some specialized data brokers that sell a variety of health-related products based on the data collected outside of HIPAA. Consumer lists are available based on diagnosis, such as depression, ADHD, or anxiety, as well as medications used such as antidepressants [44]. Health data are also combined with data on consumer habits and demographics,
potentially making a digital profile very detailed. These data help brokers generate consumer health scores, profiling, and predictive modeling [45]. These scores used outside of the HIPAA framework include Acxiom’s Brand Name Medicine Propensity Score and the FICO Medication Adherence score [46,47]. Life insurers may use consumer health scores as variables within predictive models as part of an evaluation process [45].

In the United States, there is a lack of clear categorization distinguishing data brokers as a distinct type of business entity [48]. Instead, various classifications exist, such as “data processing and preparation”, “credit reporting services”, and “information retrieval services”. The Federal Trade Commission (FTC) defines data brokers as “companies that collect consumers’ personal information and resell or share that information with others” [49]. However, this definition encompasses many organizations that engage in the commercialization of personal data and may not specifically align with the conventional understanding of data brokers [48]. Furthermore, states have differing definitions of data brokers. For example, in California, Vermont, Oregon, and Texas, data brokers are defined as companies that do not have a direct business relationship with consumers and are responsible for the collection and use of information through other sources (third parties) [50]. While the exact definition may be subject to debate, it is widely acknowledged that these entities depend on acquiring, utilizing, and processing personal data obtained either through scraping public records or publicly available sources, or by purchasing datasets from various sources [48].

The industry of data brokers operates with minimal oversight and regulatory control, lacking federal legislation in the United States. Today, with the increasing integration of AI in business operations, there is a pressing need for enhanced policies and regulations governing marketing data [51]. While some states, such as Vermont and California, have taken steps to regulate data brokers, including measures like mandatory registration with the Secretary of State, disclosure of activities, consumer opt-out options, and stricter oversight of data breaches [52], it is imperative that similar initiatives be adopted across all states to ensure comprehensive protection and accountability. Concerns about health data related to reproductive rights emerged in the wake of the Supreme Court of the United States’ decision to overturn Roe v. Wade. Many wearables and health apps collect data on women’s menstrual cycles and fertility, raising concerns about privacy and the potential misuse of this sensitive information [53]. The concerns are driven by the fear that personal data collected from wearables and health apps, among others, could be used to penalize individuals seeking or considering getting an abortion in states where it is illegal given their current condition [54]. These concerns have been vocalized among privacy advocates, asking users of menstrual apps to delete their data and uninstall the apps [54]. The main challenges with menstrual and health apps are the intimacy of the health data being collected by a technology not considered to be health-related [55]. Apps, like Flo, a menstrual-tracking app, ask users to disclose their symptoms as well as their mood and emotional well-being [56]. All these data are pieced together to create a “user-friendly” and tailored experience by providing personalized recommendations and tracking of the user’s health. Flo, or any other app or WHMD, requires users to accept the terms and conditions to be able to access these “free services”, in exchange, some of the consumer data will be shared with other third parties.

In the case of Flo Health, Inc. (London, UK) v. FTC (2021), the Federal Trade Commission (FTC) asserted action against Flo Health. The FTC alleged that Flo Health shared sensitive health data of its users with third parties, including providers such as Facebook and Google, which went against the terms of service stated by Flo [57]. Although Flo Health settled the allegations without admitting any wrongdoing, they agreed to obtain affirmative consent from users before sharing their health information, conduct an independent review of their privacy practices, and notify affected users about the unauthorized data sharing while instructing third parties to delete the data. Following the settlement, the FTC finalized updates to the Health Breach Notification Rule (HBNR) to cover health apps and similar technologies not protected by HIPAA [58]. Changes include revised
definitions (such as changing the “PHR identifiable health information” and adding two new definitions for “covered health care provider” and “health care services or supplies”), expanded use of electronic notifications to inform users about the breaches through email, clarified breach definitions, and increased content requirements for consumer notifications (such as providing information on the identity of the organization that acquired unsecured Personal Health Records (PHR)) [58]. However, the updates made are still limited in scope.

Data can also be purchased for re-identification. This means that even if personal information is anonymized, it can still be linked back to specific individuals through other data sources. This is a major concern because the more available information about a person, the easier it is to re-identify the person in the future [59]. Additionally, while data brokers argue that data are anonymized, research has found that what they claim is anonymous is easy to de-anonymize. It takes as few as fifteen characteristics, which include age, gender, etc., to re-identify a person with 99.98 percent accuracy [60]. This reverse engineering presents the gaps of a broken ecosystem of ad tech and the lack of regulations that protect the privacy of consumers. Indeed, data broker scrutiny has been increasing in recent years as policymakers grapple with the ethical and regulatory challenges posed by the widespread collection and monetization of personal information. With the lack of a federal privacy framework geared to consumer data and the lack of the regulatory oversight of data brokers, WHMDs are left to operate in a murky and exploitative landscape.

3.5. Summary

Wearable health devices marketed for consumers are not considered medical devices, and thus do not require FDA approval. Additionally, while WHMDs do not need to undergo the rigorous vetting process required for medical devices, they still play a significant role in providing users with valuable health-related insights and data. The absence of stringent regulatory scrutiny may leave room for inconsistencies in data accuracy, device reliability, and user safety. When WHMDs and health apps are used for consumer monitoring purposes, the generated data are not covered by HIPAA. This misclassification allows this type of health data to be sold in the open market since it is not protected by the same privacy laws that govern Protected Health Information (PHI) per HIPAA regulations. Furthermore, the lack of regulatory oversight for selling these data undermines the information being shared, sold, and re-engineered to de-anonymize users. Adding to these issues is the lack of consumer literacy on how these technologies collect, use, and share data. The adding complexity of health literacy further amplifies the challenges faced by consumers in understanding and navigating these technologies. That said, with the growth of wearables for health monitoring and their integration in individuals’ daily lives, there is a pressing need for broader and more stringent privacy regulations to ensure the protection of this sensitive information.

4. A Framework for WHMDs and Consumer Health Apps

Based on previous research, this paper proposes a framework that categorizes various types of data and offers solutions that address the current gaps. Figure 1 shows the suggested framework.
by consumers in understanding and navigating these technologies. That said, with the growth of wearables for health monitoring and their integration in individuals daily lives, there is a pressing need for broader and more stringent privacy regulations to ensure the protection of this sensitive information.

4. A Framework for WHMDs and Consumer Health Apps

Based on previous research, this paper proposes a framework that categorizes various types of data and offers solutions that address the current gaps. Figure 1 shows the suggested framework.

**Figure 1. A framework for WHMDs and consumer health apps.**

4.1. The Problem

First, we identify the problem that is caused by WHMDs. More specifically, this paper investigates the phenomenon of individuals using wearable devices that integrate apps or algorithms that collect, use, and share health monitoring data. These wearables include fitness trackers that collect data on physical activity and monitor heart rate and sleep patterns, etc. An example of this could be an individual using FitBit or Apple Watch.

4.2. Data

Once an individual starts using WHMD, it is important for users to be able to recognize if their device or app is FDA-approved. In fact, data that are generated through wearables (including the apps/algorithms that are used to analyze the data), may or may not meet the FDA's standards, and this has implications on their usage for medical and clinical purposes. Such data, meeting regulatory requirements, become a valuable resource that can be used by healthcare professionals and even for research purposes. However, non-compliant data collected from wearables lack the necessary adherence to FDA guidelines. Therefore, these data are limited in their utility for medical purposes and potentially pose risks to validity and reliability.

Considering the blurred distinction between sensitive health data and less critical lifestyle data, adopting a one-size-fits-all approach to handling health-related personal data would be misguided. Applying the rigorous privacy, security, and safety standards typically reserved for medical devices (i.e., needing FDA approval) and healthcare data to all health-related personal information could render numerous commercial fitness devices unsuitable for everyday consumer use. However, overlooking the sensitivity of wellness data by treating it as generic personal information, would also be an oversight.
4.3. Data Transfer

When it comes to data transfer, it is important to recognize the various pathways through which data can move between different entities. For example, when these data are transferred to a HIPAA-compliant party, such as healthcare providers or insurers, HIPAA regulations apply. This ensures that the handling of personal health information complies with stringent privacy and security standards mandated by HIPAA, safeguarding patient confidentiality and preventing unauthorized access or disclosure of sensitive data. However, when those data flow to a non-HIPAA compliant party, problems arise. In fact, when WHMD data move to parties not bound by HIPAA regulations, the risk of privacy violations and infringements increases as these parties are not bound by HIPAA liability, including the Privacy Rule and Security Rule.

Moreover, data transfer to non-HIPAA parties for resale raises additional concerns regarding the potential exploitation of personal health information for commercial purposes. Without strict regulations and oversight, there is a risk that third-party entities may collect, aggregate, and sell health data to other parties without the user’s explicit consent.

4.4. Solutions

4.4.1. Federal Framework for Health Data Generated by WHMD for Consumer Use

In 2023, the state of Washington enacted the My Health My Data Act (MHMD), which represents a significant advancement in the regulation of consumer health data privacy [61]. This legislation, which took effect on 31 March 2024, introduced strict requirements for obtaining explicit consumer consent before the collection or sharing of health data by regulated entities and small businesses [61]. In fact, this new regulation addresses the gaps of existing frameworks such as HIPAA, as it extends the protection of health data, including that collected by non-covered entities, like certain applications and websites. Furthermore, this new regulation empowers consumers with the right to access, delete, and manage their health data [61]. MHMD also prohibits the sale of consumer health data without valid consent and limits the use of geofencing technology in proximity to healthcare facilities [61]. This new legislation highlights the increasing recognition of privacy as a fundamental right and the need for rigorous safeguards in the digital age, especially when it comes to consumer health data. While the MHMD Act is a pioneering step for Washington, it underscores the need for similar comprehensive federal regulations to ensure consistent protection of consumer health data across all states.

Safeguarding consumer privacy and preventing misuse of personal information should be enforced with a federal framework that establishes clear and strict guidelines for data collection, storage, and sharing. The federal framework should delineate clear guidelines for the collection of health data generated by WHMDs and health apps, specifying the types of data that can be collected and the methods by which it can be obtained. While it is not feasible to apply the same stringent regulations used for medical data to all health-related information, it is crucial to recognize the sensitivity inherent in the data generated by consumer health monitoring devices and health apps. As such, there is a need for a federal framework that acknowledges this nuance and provides appropriate safeguards for personal health information. This manuscript emphasizes the importance of implementing robust privacy regulations that encompass all types of personal information, including health data, to ensure the protection and privacy of individuals’ sensitive information. Moreover, this framework should enhance oversight through holding organizations accountable for the responsible use of consumer data and preventing potential abuses.

4.4.2. Data Brokers Regulation

The pervasive data collection practices employed by data brokers and technology companies have raised concerns about privacy and security among consumers and policymakers in the last decade. Justin Sherman, a specialist in data brokerage, who recently conducted research revealing the sale of sensitive military personnel information by data brokers without due diligence, expressed astonishment at the proliferation of companies...
selling data pertaining to minors [62]. “As Congress fails to do its job in this area, states should pursue strong data broker regulation”, Sherman said [62]. The sheer amount of personal information being collected on individuals keeps challenging current privacy laws and regulations. According to a study conducted by the Federal Trade Commission (FTC), a single segment of data brokers possessed records pertaining to 1.4 billion consumer transactions and an extensive dataset comprising over 700 billion raw data elements [52]. Furthermore, according to the World Privacy Forum, the average data broker has information on approximately 1500 data points for every consumer. That is potentially 1500 tidbits of information on one individual [63]. The business models of these organizations rely on personal information; therefore, abolishing or significantly restricting their data collection practices could potentially disrupt their operations and revenue streams. The media buying business model that underpins the advertising industry relies heavily on the extensive datasets furnished by data brokers. These datasets are pivotal for advertisers to customize and disseminate targeted promotional messages to specific consumer segments, ensuring optimal impact. However, a need to revisit and strengthen data broker laws to protect consumer privacy and data security is becoming increasingly apparent in an age that keeps advancing in technology and data collection capabilities.

The urgency of regulating data brokers is becoming increasingly critical as the consequences associated with their practices continue to escalate. In a recent case, Near Intelligence, a data broker, was found to have geo-tracked visits to approximately 600 Planned Parenthood locations across 48 states and sold these location data to an anti-abortion group [64–66]. This group then used the data to run targeted anti-abortion campaigns based on the location-based information. These campaigns involved sending ads with anti-abortion content to individuals who had visited these clinics [64–66]. This recent case highlights the ongoing issue of not recognizing certain data, like geographical location, as health information when they are used as such. The invasion of privacy, and the profiling of individuals through access to their information amplifies the risks and harms created by the unregulated data brokerage ecosystem.

In summary, if the use of digital technologies continues to proliferate in the health space, it is crucial for the U.S. Congress to include data brokers in a comprehensive federal privacy framework. This legislation should clearly define regulations and impose strict limitations on how data brokers collect, aggregate, sell, and share personal data. Furthermore, it is crucial to enhance the Federal Trade Commission’s authority to scrutinize and rectify unethical and exploitative activities conducted by data brokers, as well as the utilization of brokered data by other entities.

4.4.3. Mandate FDA Approval and/or Regulatory Oversight

This current paper advocates for the mandating of FDA approval for data from wearables used for health monitoring. The FDA, as the regulatory authority responsible for ensuring the safety and efficacy of medical devices, plays a pivotal role in safeguarding public health. While FDA approval is primarily reserved for medical devices or wearables with capabilities comparable to medical devices, imposing this requirement on every device may not be feasible. However, it is crucial to establish oversight for any device or health app using health monitoring data and providing health-related information to consumers. This oversight should focus on ensuring the reliability and credibility of the information provided, especially considering that consumers may make health decisions based on these data. Furthermore, given the potential sharing of data with third parties, such as data brokers or advertisers, maintaining accuracy and reliability becomes paramount to safeguard consumer interests and privacy. Therefore, while not every device may require FDA approval, establishing oversight mechanisms to uphold the accuracy and reliability of health information shared with consumers is essential.
4.4.4. Increase Consumer Digital and Health Literacy

A primary challenge in privacy management lies in the assumption that consumers are aware of the various ways that companies collect, use, and share data. However, studies have shown that many consumers are not knowledgeable of the extent of data collection and its implications for their privacy. To compound matters, the continued development and evolution of new technologies as well as the integration of technologies like wearables in daily life further complicates the issue of privacy management. Increasing consumer literacy related to digital media becomes crucial. However, it is also important that individuals understand the implications of using these technologies. Adding to the issues of digital literacy is health literacy. When using WHMD, individuals must rely on their ability to understand and interpret health information, which can be challenging for those with low health literacy. Health literacy, defined as the capacity to obtain, comprehend, and apply health-related information effectively, significantly influences health outcomes [67]. In fact, low health literacy is associated with difficulties in adhering to medication instructions, understanding health-related information, and making informed decisions about one’s health [68].

To address these challenges, it is essential to implement educational initiatives aimed at enhancing digital and health literacy among WHMD users. These initiatives should focus on providing clear and accessible information about the functionality of WHMDs, the interpretation of health data, and strategies for incorporating this information into one’s healthcare routine. Healthcare providers should work with their patients by demonstrating how to use the devices (i.e., apps) and explain how to interpret the collected data. Furthermore, healthcare providers should inform their patients about privacy and security risks, as well as provide a clear understanding of HIPAA and any potential liability issues if applicable. Additionally, healthcare providers should tailor these educational efforts to meet the diverse needs of different patient populations, considering factors such as age, technological proficiency, and cultural background.

Furthermore, continual technology and policy education is required for healthcare professionals with regard to current progress in WHMD technology and its application in their clinical decision making. For the technical and practical aspects of WHMD usage, comprehensive educational programs should be developed in collaboration of healthcare professionals, technology developers, and pedagogical experts. These types of efforts will allow policymakers to advocate for the availability of digital health literacy strategies and tools for all, especially those from underserved communities.

4.4.5. Improve Consent and Design Transparency

Consent legitimizes the collection and use of personal data by the organization and third parties [33]. Specifically, the notice and choice process give consumers a set of rights that allow them to have control over their decisions regarding personal information. These rights include the ability to know what information is being collected, how it will be used, and who it will be shared with [33]. However, this consent is often buried within lengthy terms and conditions agreements and thus consumers may unknowingly grant permission for their personal information to be collected and shared without fully understanding the implications [33,35,36,69].

The primary theoretical lens that has been applied to the relationship between consent and privacy, is the privacy paradox [43,70,71]. The privacy paradox looks at this disconnect between users’ privacy concerns and their behaviors [43]. Research on the privacy paradox has shown that consumers might judge privacy as important but still continue to exhibit careless behaviors by engaging in self-disclosure (e.g., voluntarily sharing personal information publicly, disclosing personal information to unverified websites or apps) [71,72]. This research has led businesses to believe and work under the idea that consumers value access over privacy [73]. In order to move forward and enact greater privacy, on behalf of consumers, a new approach to studying consumer responses and understanding their interactions with digital media, such as consenting to terms and conditions including data
access becomes crucial. Scholars argue that looking at these interactions as a social contract could provide a better understanding of the complexities of privacy and the nuances of digital contracts. Martin defines the social contract as “negotiated information norms within a particular community or situation” ([73] p. 520). This concept stems from the social contract theory, which posits that individuals enter into implicit agreements or contracts with each other to establish rules and norms for their interactions [74]. The concept of a social contract recognizes that privacy is a dynamic agreement between consumers and organizations, encompassing not just the legal compliance illustrated in the consent given but also in consumers’ understanding of that consent [73,75–77]. Privacy as a social contract offers a new approach that investigates consumers’ privacy protection behaviors. This perspective argues that users have a responsibility to actively participate in the protection of their own privacy. Indeed, this approach seeks a more balanced relationship between individuals and organizations by recognizing the importance of organizations implementing robust privacy measures while also acknowledging that individuals must take proactive steps to safeguard personal information. The social contract encourages consumers to be more vigilant about the data they share, educate themselves about privacy policies, and make better choices about the platforms and services engaged. Thus, this manuscript recommends studying the concept of privacy as a social contract to promote consumer literacy and efficacy related to digital contracts, highlighting the implications of their consent and the importance of proactive privacy protection.

On the practical level, it is recommended that organizations ensure full transparency regarding the approval status of the data they collect or their programs—specifically, whether it is FDA-approved or not. This clarity is crucial for consumers to understand the rigor and accuracy involved, especially if they are relying on the data to make health decisions. Furthermore, organizations should be transparent about how data are shared and with whom. This should include potential consequences of organizations using the data as a means to classify or de-anonymize the user. Wearables should provide clear opt-in/opt-out and delete options for users to control the sharing of their data, as well as regular updates on how their data are being handled. Finally, if sharing involves parties covered under HIPAA, this information must also be clearly communicated to consumers.

Furthermore, this manuscript highlights the importance of Privacy-by-Design (PbD) when it comes to WHMD. The design of WHMDs should prioritize user-friendly interfaces and intuitive features that accommodate users with varying levels of digital and health literacy. This includes simplifying data visualization, providing contextual explanations of health metrics, and offering personalized recommendations for improving health behaviors. Furthermore, consent forms, opt-ins, and opt-outs should favor users’ understanding of how their data will be used and shared, as well as giving them the tools to easily manage and adjust their privacy settings.

### 4.4.6. Improve Security

The HIPAA Security Rule plays an important role in protecting electronic Protected Health Information (ePHI) by establishing national standards for its security [78]. As stated, HIPAA requires healthcare providers, health plans, and healthcare clearinghouses to implement administrative, physical, and technical safeguards to maintain the confidentiality, integrity, and availability of ePHI [78]. The current manuscript argues that similar standards are needed for wearable health monitoring devices (WHMDs) and health apps that collect, use, and share consumer health information. This includes implementing robust encryption and anonymization techniques to enhance data security. Additionally, we propose increasing the scrutiny of the Breach Notification Rule, which mandates that covered entities must notify affected individuals, the Secretary of Health and Human Services (HHS), and, in some cases, the media, if there is a breach of unsecured ePHI [79]. As WHMDs and health apps become more widespread, it is increasingly critical to ensure they are subject to stringent security standards and oversight to effectively protect consumer health information.
5. Challenges and Opportunities

It is acknowledged that implementing the proposed framework for enhancing the privacy and security of data collected by WHMDs and health apps presents challenges. One major obstacle is the lobbying efforts of data brokers, who may resist stringent regulations that would limit their data collection and sales capabilities. In fact, data brokers have increased their lobbying activities in response to tightening privacy laws in the United States, aiming to shape legislative outcomes to their advantage. Over the past few years, these companies have spent over USD 143 million on lobbying efforts, reflecting their strategic investment in influencing privacy legislation [80]. This surge in lobbying coincides with growing legislative efforts to impose stricter regulations on how personal data is collected, used, and shared, which data brokers strongly oppose [81]. The current regulatory environment, which has been demonstrated to be riddled with loopholes, allows data brokers to exploit consumer data with minimal oversight, prompting calls for more robust protections and transparency [7]. These concerted lobbying efforts underscore the industry’s resistance to reforms aimed at enhancing consumer privacy and accountability in data handling practices.

The discrepancy between federal and state regulations can further complicate the landscape for data privacy and data broker practices. With different definitions, requirements, and enforcement mechanisms across states, nationwide businesses must navigate a patchwork of regulations, leading to higher compliance costs and operational challenges, especially for those aiming to meet the strictest state standards. This regulatory inconsistency also places a burden on consumers, who must understand and navigate varying levels of protection depending on where they live.

The framework suggested in this manuscript contributes evidence and insights that build on existing and ongoing efforts by researchers, organizations, and regulators in the field of privacy policy. The recommendations provided can be used by think tanks, consumer advocacy groups, and lobbying organizations. The next steps involve leveraging this research to inform policymakers about the critical need for updated privacy legislation. Collaborations between research institutions, NGOs, think tanks, and regulators have led to the introduction of bi-partisan bills that further aim to address challenges with big tech and privacy.

6. Discussion

The continued march of technological progress has opened up novel avenues for individuals, businesses, and entire industries. In the healthcare sector, one of the most significant advancements has been the proliferation of WHMDs. These devices range from smartwatches to fitness trackers and have allowed users to track and manage their health and wellness in real-time [1].

However, along with the benefits that these technologies offer comes important considerations regarding privacy and security of the devices and data generated. Indeed, these devices fall outside of FDA oversight since they are not categorized as medical devices. Consequently, health metrics collected by WHMDs are not scrutinized to the same level as health information, yet they reveal sensitive information about consumers. Furthermore, generated data by WHMDs raise privacy risks and potentially infringe upon individuals’ privacy rights [7]. While health data are generally protected under HIPAA, the data generated by WHMDs intended for commercial use do not fall under this set of regulations.

The lack of a comprehensive privacy framework, the current challenges of regulating the data brokers industry and the lack of oversight of WHMDs further exacerbates concerns about personal information and privacy rights. Additionally, consumers’ limited understanding of the different regulations put in place to protect them, and the inadequate notices designed for consent to share health data with third parties, contribute to the potential misuse of sensitive personal information collected by WHMDs.

The current manuscript explored these challenges and current regulatory loopholes. Through a suggested framework, this manuscript categorizes WHMD data and delineates
the various data transfers to different parties. By doing so, solutions and recommendations were outlined for policymakers, consumers, healthcare professionals and advertisers. The need to recognize the lack of proper categorization of these sensitive data highlights the urgency for comprehensive regulatory measures. Without clear guidelines, there is a risk of exploitation and misuse of WHMD data.

Today, privacy protections have become essential to our ability to be involved in a digital and data-driven world. Without taking into account the limitations of the current regulations meant to protect consumers and limit the monopolistic power of tech companies and data brokers, we are facing an unprecedented challenge in safeguarding personal information.

Author Contributions: Both authors contributed significantly to this manuscript. The narrative structure was directed by M.S.E., while A.S. provided policy knowledge and conceptualization of the arguments. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data was created.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kang, H.S.; Exworthy, M. Wearing the Future-Wearables to Empower Users to Take Greater Responsibility for Their Health and Care: Scoping Review. JMIR MHealth UHealth 2022, 10, e35684. [CrossRef]
6. Tariq, M.U. Advanced Wearable Medical Devices and Their Role in Transformative Remote Health Monitoring. In Transformative Approaches to Patient Literacy and Healthcare Innovation; IGI Global: Hershey, USA, 2024; pp. 308–326. [CrossRef]
54. Cox, D. How overturning Roe v Wade has eroded privacy of personal data. BMJ 2022, 378, o2075. [CrossRef]
70. McDonald, A.; Cranor, L.F. Beliefs and behaviors: Internet users understanding of behavioral advertising. Tprc 2010.
71. Marwick, A.E.; Boyd, D. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media Soc. 2011, 13, 114–133. [CrossRef]
74. Martin, K. Understanding privacy online: Development of a social contract approach to privacy. J. Bus. Ethics 2016, 137, 551–569. [CrossRef]
75. Dunfee, T.W.; Smith, N.C.; Ross, W.T., Jr. Social contracts and marketing ethics. J. Mark. 1999, 63, 14–32. [CrossRef]


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.