Review



# What Clinicians Should Tell Their Patients about Wearable Devices and Data Privacy

Joseph V. Pergolizzi , Jo Ann LeQuang , Salah El-Tallawy , Giustino Varrassi *

Posted Date: 19 September 2024

doi: 10.20944/preprints202409.1428.v1

Keywords: Healthcare; Wearable medical devices; people-generated health data (PGHD); Privacy; AI

*Review*

# What Clinicians Should Tell Their Patients about Wearable Devices and Data Privacy

**Joseph V. Pergolizzi [1], Jo Ann LeQuang [1], Salah El-Tallawy [2] and Giustino Varrassi [3,*]**

[1] NEMA Research, Inc., Naples, Florida
[2] Anesthesia and Pain Management Department, College of Medicine, King Khalid University Hospital, King Saud University, Riyadh, Saudi
[3] Fondazione Paolo Procacci, Roma, Italy
* Correspondence: giuvarr@gmail.com

**Abstract:** The recent growth of wearable medical device technology in the form of fitness trackers, smart watches, smartphone apps, and patient monitoring systems has created people-generated health data (PGHD) that may benefit medical science with large amounts of continuous real-world data. The prevalence of these devices speaks to their broad popularity and user-friendliness and may lead us one day to a more fully "connected healthcare system." Meanwhile, data security, confidentiality, and privacy issues have emerged in these hackable systems. Despite the promise of anonymized data, data can sometimes be re-identified, but even without that step, data breaches may reveal information (name, address, date of birth, social security number, and so on) sufficient for identity theft. Clinicians are often asked about the utility and value of wearable devices or monitors, but most are unaware that data from these systems may be transmitted, stored, and even sold without the user's specific knowledge. Despite the confidentiality of medical information, cybersecurity surrounding wearables and monitors remains relatively lax, making them comparatively easy targets for cyber-villains. It is also important that efforts be taken to make PGHD more secure, since medical data may have great value to telehealth applications and AI-physician assistants. Clinicians should take an active role in informing patients about both risks and benefits of wearables and similar devices.

**Keywords:** healthcare; wearable medical devices; people-generated health data (pghd); privacy; AI

## Introduction

Wearable medical monitors and devices ("wearables"), smartphone applications, smart watches, fitness trackers, and similar systems can be used to detect, monitor, and record health-related information, and, in some cases, relay specific alerts to clinics or healthcare professionals. Some wearables are available over-the-counter to guide individuals in health-related activities such as diet or exercise plans.[1] Implantable devices such as pacemakers may offer remote monitoring and alert systems. There are also hand-held electrocardiography devices and glucose monitors. The market for wearables and similar devices has been estimated to be worth $12 billion in 2023 and expected to increase substantially in the coming decade.[1,2] For the healthcare system, the prevalence of widely accepted, user-friendly wearables may facilitate a more fully "connected healthcare" system that links electronic medical records to wearable systems and monitors.[3] With vigorous sales proof of their popularity, people who use these devices often report a sense of empowerment.[4] Whether that empowerment is genuine or illusory is another issue.[5]

Wearables may be used for health and lifestyle monitoring; safety; management of chronic conditions, such as heart disease or diabetes; diagnostic purposes; mental health; and rehabilitation efforts. The ability of wearables to disrupt our current healthcare system and bring about positive change is clear.[6,7] Wearables may help stretch already strained medical resources by expanding access in regions with limited access to healthcare services.[8–10] From piezoelectric tattoo-like films that adhere on the surface of the skin to electronic socks, from smart watches to injectable cardiac

 doi:10.20944/preprints202409.1428.v1



monitors, the range of products is imaginative and exciting, particularly for people with a proactive approach to self-care and an openness to technological change.[11]

Wearables shift the paradigm in healthcare away from the intimacy of occasional face-to-face consultation with a clinical expert to a more continuous, more patient-centric, and more participatory model. Wearables, fitness trackers, smartphone apps, monitors, and similar systems gather a wealth of person-generated health data (PGHD). Yet few people who use these devices are aware that PGHD are inherently valuable beyond their informational content to the user. A current shortfall in the plethora of wearable innovations is a legal and ethical framework regarding how these PGHD and other data collected by these devices are stored, shared, aggregated, and utilized, as well as by whom and for what purpose.[12]

While individuals may start using wearables without benefit of physician advice, others consult healthcare professionals for advice or device selection. Patients sometimes bring wearable-generated reports with them to the clinic. Just as the clinical team works with patients to improve health literacy on disease management or wellness topics, it is important to discuss data privacy, confidentiality, and security associated with wearables. The wearable companies publish this information but make no particular effort to make sure patients understand it. The result is that people using wearables may be unaware of these issues, in particular the risks of data breaches. Many individuals tend to embed innovations in technology into their everyday routines long before they consider the consequences of privacy, data sharing, data breaches, security, identity protection, and confidentiality.

This narrative review aims to aid clinicians who may need to discuss the issues of data security and patient privacy with patients who have used or are contemplating using wearables. Google Scholar and PubMed databases were searched for keywords related to wearable data privacy. Bibliographies of relevant articles were also searched. The vast number of devices and applications made reporting on specific devices or even device categories impossible in a short review. The aim of this review is to describe how patients understand the issues of privacy with the use of wearable trackers, fitness monitors, and similar products and ways in which clinicians might raise health literacy on these important topics. In this article, the term “wearable” will be used to include not only trackers, smartwatches, and sensor-driven systems but also applications, monitors, and other systems that produce PGHD, including monitoring systems embedded in implantable systems such as cardiac devices and infusion pumps. The field is currently experiencing rapid developing, a proliferation of new devices, and a collective terms is not yet readily defined for all of these many systems.

**Results**

The evolution of how medical data are captured, organized, curated, reported, displayed, and utilized has been rapid and enormous. For centuries, clinicians collected health information in private, face-to-face sessions with patients, recording the information on paper or capturing images on film. Electronic health records brought with it digitization, improving the portability of records and allowing greater versatility in capturing and sending images, but data were still mostly obtained during individual, in-clinic sessions between a patient and a healthcare professional. By collecting PGHD rather than data reported by an individual patient or captured in the clinical setting, wearables brought a new source of health-related information that had up to now eluded medicine and public health.

With wearables, data collection is driven by patients rather clinicians, and these data can be continuous, more extensive, and better quality.[13] Wearables can collect a range of patient-related data that may be more far-reaching than patients realize. For instance, even simple fitness trackers for healthy individuals may collect other vital information, such as heart rate and respiration, as well as workout schedules, patterns in exercise, geographical locations, and lifestyle habits, such as sleep schedules.[14]

 doi:10.20944/preprints202409.1428.v1



**How Devices Collect and Transmit Data**

Wearables either collect data continuously through sensors or other means or they can collect data on demand (such as recording a workout) or manually through user input. Data are collected and transmitted wirelessly first to a user interface for organization and display, such as a sleep app that displays histograms of weekly sleep patterns. Data may also be subsequently transmitted wirelessly to a database or other repository. Wearable owners may have access to all or some of this archived information for review or reports. Data may be archived and reported historically as well.

Data transmissions generally rely on wireless or Bluetooth connections, and data are sometimes altered or modified for more efficient transmission. Data can be vulnerable to breaches during transmission, therefore, encryption is often used to safeguard data in transit.[15] While PGHD have considerable value to medical science, this sort of hacking of healthcare data is mainly committed in order to steal user identities.[16] Wearable data are attractive to cybercriminals because security provisions for such data are not always robust.[17,18] While smartphones and other data transmission systems are widely used to convey financial and private information, both the security safeguards and the deviousness of bad actors have increased almost in tandem, but medical systems have not always kept pace.[19] Thus, hacking medical devices can be a way to steal an identity and one few people consider. A summary of common hacking terms and associated risks appears in Table 1.

**Table 1.** Data security terms, hacker terms, and related dangers.[15,16,19] Terms appear in alphabetical order.

| Term | Definition |
|---|---|
| Authentication | A method of validation of data destination that confirms proper identity of data recipient |
| Breach | A broad term for any act or event where an unauthorized party can access personal, private, or confidential information |
| Eavesdropping | Real-time interception of private communications |
| Hard trust | Mechanisms such as authenticity controls, encryption, algorithms, and audits in place to harden data security |
| Interruption | Failure of data in transit to reach its intended destination, which may be due to technical problems or a hacker intervention |
| Malware | The use of dangerous viruses, worms, or other tools to corrupt data once it is in a repository (such as stored on a computer or app) |
| Message alterations | Changing the content of the data while they are in transit; this may be the content of the message or the timestamp<br>Also called data modification |
| Sniffing | Monitoring every data packet that passes through a certain checkpoint (network) |
| Soft trust | A personal and often emotion-drive perception of security and safety, often shaped by the brand and social influence of the device |
| Tapping | Using a hardware device to access data in transit |
| Traffic analysis attacks | Monitoring data transmissions from a wearable and a smartphone or software app in order to identify users or detect their activities |
| Virtual private network | A private, hidden, and restricted passageway (like a tunnel) through which data can flow |

 doi:10.20944/preprints202409.1428.v1



Patients may approach certain wearables with soft trust because of brand familiarity and/or tacit or overt endorsement of the wearable by a clinician. People may be unaware that wearables can be a "point of entry" for identity thieves. For this reason, clinicians must be able to frankly discuss data security with patients who are unaware that these devices can be hacked.

For most people using wearables, data storage is a black box—they do not know where their data are stored, how they are stored, or even who stores them and accesses them.[19] Some individuals may be unaware that the data exist outside of their devices or might have any value to outsiders. Knowingly or unknowingly, most people take a leap of faith with these wearables, assuming that their personal information and medical data are being properly secured in accordance with the law and local regulations. While safeguards exist to protect personal data in all spheres of life, data breaches are not uncommon. In 2023, over 100 million Americans were affected by a data breach, data leakage, or exposed data; it would be difficult to find an American not directly or indirectly affected by a cyberattack.[20]

A key concern with data storage is the ability of data to cross state and even country lines, in which case the laws of the destination locality would govern how the data are to be handled.[21] Regulations, laws, and practices of data storage and data protection can vary markedly among countries, so data collected under strict provisions of California law may be transmitted for storage to India, whose more lax regulations would then prevail.[22] Even if they were aware of this translocation, users may not be able to prevent their data from being moved to more lax locations. In fact, users may not be able to ascertain even where their data are stored. Compounding the problem, the same data may be placed in multiple repositories.

A typical wearable collects PGHD, transmitting these data to an application (for user review and examination) but also sending encrypted data for storage to a company-owned database. Hacks and data breaches of that database can expose all data.[23] An important example of the risks of how vulnerable seemingly innocuous devices can be involves Strava, a fitness wearable that uses heat maps to track activity patterns. In the Syrian war zone, the Pentagon discovered that a hack of Strava revealed the positions of U.S. military facilities in Syria and Iraq and even certain troop movements.[24] While war zone examples may not be relevant to the average patient, it is important to know that the data collected by wearables are stored and may be hacked for nefarious purposes.

**How Data Are Used**

Besides concerns about hacking, people who use wearables may be unaware that data from their medical devices may be used by third parties without their express permission. PGHD possess real scientific value and can be sold as such. While legitimate investigators would not utilize PGHD in this way, this does not mean there is no market for such data. A survey of 842 people who used wearables asked respondents if they would be amenable to selling their personal data for various price points. A bimodal distribution occurred, suggesting that the sale of such data might be socially divisive, because some respondents considered the data of little value, while others wanted high payments.[25] In a survey of 1,300 American wearable users, most were willing to share their health-related data with their clinical team (82%).[26] Most wearable users are not aware that third parties may have interest in their data as well.[19]

Ideally, when PGHD arrive at their destination database, they are anonymized or de-identified and arrive in packets, so that specific information cannot be tracked back to the individual owner. This may provide wearable users with a false sense of security, because retrograde processes can "re-identify" data by finding clues to link anonymized data back to their origin, with success rates as high as 86% for certain cases involving wearables. The re-identification process need only take a short run < 5 minutes of live data from the device to use things like the electrocardiogram, heart rate, respiration rate, gait, or other factors to match allegedly de-identified data with their owner.[27] While this would rarely be used to identify random individuals, it is possible that specific data from a specific user might still be traceable.

Wearables are a novum in medicine, and that means that privacy issues have yet to evolve into nuanced options for device owners. Ideally, wearable owners should be able to opt out of data

 doi:10.20944/preprints202409.1428.v1



collection, but not all devices allow this and not all consumers would demand it. Wearable users have few if any ways to confirm whether their data are being collected, by whom, and where this information is stored. Even the United States government has few ways to hold companies responsible if they collect data on unwilling subjects.[27]

PGDH are often shared, sold, and distributed to third parties without the knowledge or consent of the wearable owners.[28] Although not a wearable system, a good case in point is the proliferation of DNA-testing services, which altogether hold genetic information on tens of millions of people. These DNA-testing companies are not obliged to follow health insurance portability and accountability act (HIPAA) regulations, because they are considered neither healthcare providers nor insurance companies. Nevertheless, genomic data stored by these companies are sometimes sold to companies for medical research.[29] To protect the medical public, the Data Sharing Hierarchy (DASH) guideline was compiled following a hierarchy of threats to patient privacy.[30] While offering only a framework, the goal of DASH was to bring a degree of risk management to PGHD collection. A crucial finding of DASH was that as technology improved, risks to patient privacy increased.[30]

**Who Owns PGDH?**

PGHD offers an abundance of real-world patient data and their value would be hard to overstate. Nevertheless, PGHD remain inadequately defined and understood, in particular with respect to the issues of data privacy and security.[13] In the future, PGHD may make digitized clinical trials possible and offer scientific researchers the possibilities of “digital twins” for drug development. Medical companies may use PGHD in developing new products or refining existing products and services. Insurance companies could employ PGHD to more accurately devise beneficial wellness programs and assess risk for various health conditions. Public health organizations can use PGHD for population health assessments, public health interventions, and contact tracing. Regulatory bodies may use PGHD for post-approval surveillance, safety monitoring, and even to contribute to the development of medical guidelines.[13] It is possible the utility of PGHD goes far beyond this.

The ownership of PGHD pose new questions that individual nations or even individual states within the United States may resolve differently.[31] While an individual can clearly own a wearable device, the data are another question, rarely addressed in scientific literature. The issue is murky even going back to the old days of color-coded paper medical files filled with handwritten notes and records. These were considered to be professional medical opinions and thus “original works of authorship” which the physician (or healthcare system) rather than the patient owned.[32] Of course not all states are in agreement and New Hampshire, for instance, specifically states that patients own their own healthcare data; many states are quite silent on the subject.[32] This poses the thorny issue of how a physician or healthcare system that owns healthcare data as “original works of authorship” is then obliged to protect the privacy of patients. For many people and even legal authorities, the issue is more about access than ownership.

In the United States, once data are de-identified, HIPAA restrictions no longer apply.[32] Large de-identified datasets can be very valuable and are sold to researchers. For example, a drug company may want records on how patients respond to their particular product. Owners of de-identified datasets can sell these data, but patients get no remuneration.[32] In fact, most patients have no idea that their medical records contribute to large medical databases that are bought and sold.

Explaining medical privacy to patients can be challenging, because the legal and medical arguments are convoluted and sometimes strange, such as the long-standing trope that patients own “the information” in their records but the provider owns “the record itself.” Digitized data from wearables makes this even more challenging for patients to grasp.[33]

However, PGHD or wearable data pose a new legal challenge. Generally, wearable manufacturers stipulate that the data collected by their devices belong to the manufacturer and that the manufacturer is granted broad discretion in terms of what to do with these data.[34] When Google acquired Fitbit in 2019 for over $2 billion, it was speculated that the purchase was made not to buy

 doi:10.20944/preprints202409.1428.v1



the relatively straightforward fitness tracker technology but rather to acquire the health data of millions of regular Fitbit users.[35]

**Looking Ahead: When AI Met PGHD**

Artificial intelligence (AI) requires vast amounts of data to build its large language models, and data from wearables may in part feed the machine building healthcare AI. On the one hand, this may open the door to personalized medicine, cheaper digitized clinical studies, improved patient safety with remote monitoring, and other advantages. Virtual physician assistants are possible with AI. Telehealth applications can be radically expanded and made more personalized.[36] At this point, AI is more of a clinical possibility than a clinical reality, but the potential for AI expansion into healthcare is undeniable and will no doubt take shape quickly in the coming years.

The stumbling blocks to greater expansion of AI are currently being sorted out, including privacy rights and technological challenges. Medical data are not collected in a standardized way and data from wearables are generally offered raw rather than in an efficiently curated package.[37] The development of healthcare AI is going to require more standardized data collection, better privacy controls, and overcoming clinical reticence to using AI in this way.[37] The interest of Google in both AI systems and PGHD from Fitbit is a good illustration of how AI will evolve.[35]

Healthcare AI will clearly disrupt healthcare system. AI chatbots could be used as virtual physician assistants that offer more in-depth telehealth interactions with patients on lifestyle modifications, disease diagnoses, medications, and consultations. Genetic information interpreted with AI may benefit research applications, because AI can be used in drug development and even to conduct AI-style research studies. Finally, physicians and other healthcare providers can benefit from AI in terms of interpreting complex medical images, reviewing and analyzing data relevant to complex cases, and sorting through vast amounts of data quickly.[37] For example, AI is already used widely in electrocardiogram interpretation when Holter monitors capture hours of tracings.[38]

Since AI or machine learning (ML) is a fast-moving and emerging new field, cyber experts must keep pace with privacy concerns as techniques advance.[39] Right now, it appears as if AI will expand more rapidly into healthcare than patient privacy protections. AI seems particularly useful for translating large datasets into meaningful results, but it is imperative that the data can be safeguarded along the way.[40]

**Patients' Perceptions of Data Privacy**

Wearables are a global phenomenon but there can be national and cultural distinctives in terms of how privacy is defined or valued. In a survey conducted in China (n=2,058), 52% of respondents had experience using some sort of wearable, but most had only low levels of understanding of what the device did, how it worked, or privacy issues.[14] In a survey of 1,005 European consumers who were asked about wearing a smartwatch that would monitor them continuously for evidence of a potential cardiac arrest to facilitate timely intervention, 90% were interested in the technology and 75% said they would be willing to wear such a watch, but their main concerns were privacy, data protection, and device reliability and accessability.[41] In a survey of 550 participants in Germany, 34% said they already wore a smartwatch or some sort of fitness tracker and 61% were open to data sharing, although concerns about privacy and data security were raised.[42]

Even when wearable manufacturers offer detailed privacy policies, patients and clinicians remain largely unaware of how or why PGHD are being used. Furthermore, wearable owners are often oblivious to the fact that, once their data are collected, third parties may further disseminate their data.[19] In other words, the wearable company may sell user data to one company, who may in turn share it with a university, which may then grant access to that data to another research organization. The user has no control over these data-sharing cascades. Regulations may be beneficial, but consumer-grade devices like fitness trackers or health applications are not regulated to the same standards as medical devices, if they are regulated at all.[43]

When a healthcare provider, hospital, clinic, or other suggests the use of wearables, this may be perceived by the patient as an endorsement and an assurance of data protection.[44] Thus, the use of

 doi:10.20944/preprints202409.1428.v1



wearables may require a conversation about the cornerstones of medical privacy, confidentiality, and security. Medical privacy is a complex subject that defies easy definitions and privacy is often blurred with confidentiality and security. See Table 2.

**Table 2.** Open questions involving the privacy, confidentiality, and security in wearables and other health-related devices that collect PGHD.

| | **Privacy** | **Confidentiality** | **Security** |
|---|---|---|---|
| Key questions | Who has access to the information?<br>Under what conditions may the information be accessed? | Are there any limitations on what data may be collected and where/how? | What measures are being used to prevent unauthorized access, use, modification, or dissemination of my data?<br>Are data encrypted? |
| Domains this affects | How and where are data stored and transmitted?<br>Is personal information (name, address, birthdays, identification) collected? | What third parties (if any) can access the data?<br>What laws are involved if data crosses borders? | What ways are there to protect against computer hacks, data breaches, unauthorized data disclosures? |
| Other issues | Can data collection be prevented in some cases?<br>Are there limits to what type of data is collected? | Can a clinician share data without permission if it is de-identified? | Security authorizes who can access data, but who controls the actions of the authorized users? What limitations (if any) may affect authorized users? |
| Data owner | Who owns the data? | How does the manufacturer protect the user's privacy? | How does the system secure the data? |
| Crucial points to consider | Who may sell the data? | Can the wearable owner limit data collection of particularly sensitive information (mental health issues, pregnancy, cancer)? | What techniques are used for cybersecurity? |

Many patients are concerned that sensitive or personal health-related information might be used in ways that could cause discrimination, such as information about disease diagnoses, mental health conditions, substance use disorders, and so on. Prospective employers, universities, insurance customers, social service offices, and others could be influenced adversely by such information. Minorities and transgender persons in particular were afraid that unauthorized use of their data might have negative consequences for them.[45] In a survey of 1,000 patients, 92% of respondents said that they had a right to privacy with their health data and such data should not be available for purchase by third parties. In this survey, 80% of patients wanted to have a way to opt-out of sharing

 doi:10.20944/preprints202409.1428.v1



their data with companies and 75% said no health data should be shared without a prior opt-in by the patient.[45] These patients are likely unaware to the fact that such data sharing is likely already going on.

**Health Literacy of Patients on Wearable Privacy**

Most wearables provide a lengthy privacy policy, which is typically difficult for laypeople to understand. Users rarely read such documents and when wearables use small screens like a watch face or a smartphone screen, the small font can make reading these texts cumbersome.[19] In a convenience sample survey of 106 participants who used some sort of wearable medical or fitness application (45% had a smartphone app, 31% an Apple watch, and 24% a Fitbit), 53% said they did not know how their device transmitted, stored, labeled, or handled their personal information. Moreover, 28% did not realize that health-related information was considered confidential or private. Data protection policies were familiar to 52% of respondents; however, 57% did not know what to do or whom to contact if they had questions about their data privacy, confidentiality, or security.[19]

Patients should be informed that their data are likely owned by the device manufacturer, who de-identify and collect these data; patients should also know that manufacturers very likely share or sell their data. This can be surprising to patients who may regard their data of little to no commercial value. Privacy policies and terms and conditions may report that wearable data are "de-identified" or aggregated and anonymized, but this may provide a false sense of security, because data can be re-identified under certain conditions and re-identification is not as difficult as it sounds.[46] Thus, it is important to emphasize that anonymized or de-identified data are important forms of data safety, but do not confer absolute protection. Patients should also be aware that genetic testing services have control of their genetic information but are not as regulated than wearables since their service is not considered medical.

Clinicians should inform patients that the theft of medical information is a form of cybercrime that is mainly used in identity theft; this type of theft of medical information is increasing at a higher rate than other forms of cyber-stealing.[37] Users may erroneously believe that all a cyber-thief can steal is their fitness data, such as steps walked per day or sleep logs; they may not be aware that device hacks can result in stolen identities, which often results in financial loss.[37] Medical records may contain names, addresses, dates of birth, social security numbers, and possibly credit card or other personal information. Just to put this in perspective, from 2005 to 2019, there were 249.9 million data breaches of all kinds.[39] Users of wearable devices should be alerted that these data security issues affect wearables as well as credit cards or bank information, although the latter often have more extensive security measures and entire cybersecurity departments at work.

Many people own and use wearables with little awareness of legibility, the industry term for informing people that their data are being collected and how they are stored.[39] Most application-based wearables rely on two sets of applications: one on or in the device itself and a companion application that resides on the smartphone or computer of the user. A study of 150 wearable applications found that 28 of them allowed sensitive information to flow across the applications, making the data vulnerable in transit. Further, in a survey related to this study of 63 wearable users, 66.7% did not know that there was a possibility for cross-device sharing of sensitive information.[47]

**Clinical Considerations**

Clinicians must be mindful that their recommendation for the use of a wearable device or monitor is often perceived by the patient as a recommendation of the use of this technology and, by implication, the assurance that these devices are safe and protect their data. Therefore, clinicians should take care to recommend devices only after they review the privacy protection information or, if recommending a type of device rather than a specific product, what privacy considerations might be. Such recommendations may be a good starting point for a short conversation with the patient about data security.

Physicians should also explain that just like banks, credit card companies, and other businesses, personal information may come to be in possession of third parties. In many cases, the user will not

 doi:10.20944/preprints202409.1428.v1



know who this is or have any way to contact that party. A risk in having data stored by third parties is that data breaches can facilitate identity theft. While this is a frightening prospect, this risk exists for most data repositories in our digital age; it is not unique to healthcare, although healthcare is not immune from it, either.

Besides hacking to obtain personal and financial information, medical information can be sold. For instance, data may be stored at a company who then sells information to advertisers seeking to reach patients with a specific condition or of a specific age. For instance, a clinical trial recruiting participants with type 2 diabetes in a specific geographical area may be able to buy lists of such people and their social media accounts for targeted advertising. Similar tactics are used outside healthcare, for instance, a preschool may buy data from local people with preschool age children at home. This type of targeted advertising may seem intrusive, but it is widely used and not just in healthcare. It is unlikely that such targeted advertising will be challenged by American legal systems.

Patients may feel comfortable with physicians, hospitals, and healthcare organizations storing their data, but may feel far less comfortable if social media companies or businesses get access to that same data.[45] Physicians should explain who might have access to their data and for what purpose and explain that wearable owners have little to no say in who has access to their anonymized data.

Some patients may resist sharing any data, a position that is increasingly untenable in our modern internet era but one that nevertheless deserves respect. For such patients, it may be important to provide the information and then allow them to decide if using a wearable device is worth the risk or not. In other words, some patients may feel that using a wearable device or telehealth app is too risky. Thus, in discussing the issue with patients, clinicians must strike the right balance between informing the patient about real risks without unduly alarming them and possibly depriving them of the benefits of wearable systems. See Table 3.

**Table 3.** Key considerations in discussing the risk of wearables and other patient devices with patients.

| Talking Points | Risk Mitigations | Risks |
|---|---|---|
| Wearables collect data and these data are owned by the manufacturer | Data are often anonymized and de-identified | Data can be breached<br><br>Identity theft is possible with some systems |
| Data may be shared or sold to other organizations, universities, and research centers | Data are often anonymized and de-identified<br><br>Such data-sharing may have scientific purposes | Even when data are sold, patients get no remuneration |
| Data may be stored in any number of locations, including overseas. The privacy laws of the place where the data are located are the ones that are in force | Data are often anonymized and de-identified. | Patients most likely will not be able to find out where their data are stored<br><br>Patients will not be able to remove their data or prevent their data from being stored in specific locations or databases |

 doi:10.20944/preprints202409.1428.v1



| | | |
|---|---|---|
| Health data are being used for AI and other systems to improve healthcare | Your data may be valuable to help build better systems | Patients will not be recognized or compensated for the use of their data |
| Wearables and their manufacturers may not have as robust security as other organizations, for example, credit card companies or banks | Systems to protect against identity theft, such as online services, may provide a degree of protection | No form of identity protection is fool-proof and vigilance is recommended |

**Can Clinicians Make Things Better?**

Numerous proposals have been discussed to better protect patient privacy. For example, it has been proposed that noise could be artificially added to certain data from patients which would make it more difficult to re-identify.[48] The drawback to this approach is that it works mainly on one aspect of the data, for instance, respiration rate or serum glucose, and not on multiple factors. It is possible that this type of security measure could be further refined and improved. Another proposal asks that those collecting wearable data do not report individual data but rather report ranges, but such an approach might limit the utility of these data for certain types of research.[27] Access to de-identified data could be restricted, but this may end up restricting access to valuable data to deserving entities.

Cybersecurity is a global concern and impacts most industries, although healthcare has lagged behind other industries in implementing robust security. Financial institutions, credit card companies, and cell phone services offer tighter security than most medical databases. This is paradoxical, since medical data enjoy exalted privacy rights outside of the cyber realm, but data protections for medical data are limited, making wearables and other such data a particularly inviting target.[49] This is particularly true in some specialistic area, as pain management, involving extremely fragile patients.[50] New initiatives, regulations, and even legislation are needed to bolster patient security as well as better countermeasures to meet attacks.[51]

The discussion about data privacy and security likely will begin with the healthcare professional who should alert patients to potential concerns without unduly alarming them. Just as Informed Consent alerts patients to risks as well as benefits of medications or procedures, clinicians should inform patients that even the most popular and seemingly harmless wearables are vulnerable to hacking and that their data may be collected, stored, shared, and even sold without their knowledge or consent. Many patients are unaware that their data have value or that seemingly benign medical information may be hacked in identity fraud schemes. Broader public awareness of these risks may expedite legislation and reforms to harden medical data, particularly as so much data are now being driven directly by patients into the healthcare system.

**Discussion**

The burgeoning use of wearables speaks to a desire of patients to be more health conscious, more proactive in their own lifestyle choices, and more empowered in healthcare. By and large, users of wearable devices are going to exhibit a degree of healthcare literacy that exceeds that of the average patients. The lacking element may be digital literacy, the next frontier in patient education.

Healthcare professionals should be at the forefront of explaining the risks and benefits of wearables to patients, many of whom are not aware that the manufacturer owns wearable data or why such companies are eager to collect vast amounts of medical data. Patients may erroneously think that their data are stored only in their device and have no intrinsic worth to third parties. Finally, people using wearables may not be aware that data hacks can compromise their personal data and expose them to identity theft.

 doi:10.20944/preprints202409.1428.v1



None of these facts necessarily preclude the use of wearables and there are mitigations against these potential risks. What is lacking is the willingness of healthcare professionals to bring up the unexpected topic of data security with their patients, to explain things frankly, and to field questions about medical privacy. There are certain aspects of wearable data privacy that may not be subject to change or mitigation: the data belong to the manufacturer, the data can be sold or shared at will, de-identification of data is not foolproof, and laws governing how medical data are to be handled vary widely among states and nations. These issues cannot be solved at the level of the healthcare system; they are political topics. However, clinicians should still be able to discuss them with patients.

Health literacy today must encompass a degree of digital literacy as well. This is not as daunting as it may seem. People of all ages routinely use digital applications for their financial transactions, business emails, and social communications; these systems are not as foreign or fearful as they might seem. Younger patients, in particular, have grown up with internet-based tools. The biggest drawback is that wearables are so ubiquitous and user-friendly that many patients may not consider that they are vulnerable to hacking and that the data they record on these systems belongs to the manufacturers. Thus, healthcare professionals must be prepared to explain these risks to patients.

## Conclusions

Wearable devices that collect PGHD have the potential to disrupt medicine and bring about many beneficial advancements such as virtual physician's assistants, digitized clinical trials, digital twins for drug development, and better understanding of health and medical trends in the form of large datasets of continuous real-world data. Wearable devices are popular and ubiquitous but they may pose risks to patients in the form of data privacy, confidentiality, and security. While medical data are highly protected, the systems, laws, and regulations to secure them are not robust or well developed. Even the question of medical data ownership is not entirely clear. Clinicians must elevate digital literacy as well as healthcare literacy among patients to assure that patients know the risks as well as benefits of using wearable devices.

**Author Contributions**: JALQ has prepared the initial draft of the manuscript. All the authors have largely contributed to review it and provide the final text, which is accepted as final by all for potential publication.

**Funding**: No funds were received for the preparation of this manuscript.

**Ethics**: This manuscript is completely based on previously published material, and it is not involving studies on humans or animals made by the authors of this research without a permission of ethics committees.

**Acknowledgments**: The Authors are grateful to NEMA Research group for the support during the manuscript preparation. They are also grateful to the Fondazione Paolo Procacci for supporting the publishing process.

## References

1. Lu L, Zhang J, Xie Y, et al. Wearable Health Devices in Health Care: Narrative Systematic Review. *JMIR Mhealth Uhealth*. Nov 9 2020;8(11):e18907. doi:10.2196/18907
2. Future Market Insights. Wearable fitness technology market snapshot (2023 to 2033). Future Market Insights,. Accessed August 9, 2024. https://www.futuremarketinsights.com/reports/wearable-fitness-technology-market#:~:text=Future%20Market%20Insights%20%28FMI%29%20projects%20the%20wearable%20fitness,contributed%20to%20the%20demand%20for%20wearable%20fitness%20devices.
3. Loncar-Turukalo T, Zdravevski E, Machado da Silva J, Chouvarda I, Trajkovik V. Literature on Wearable Technology for Connected Health: Scoping Review of Research Trends, Advances, and Barriers. *J Med Internet Res*. Sep 5 2019;21(9):e14017. doi:10.2196/14017
4. Kang HS, Exworthy M. Wearing the Future-Wearables to Empower Users to Take Greater Responsibility for Their Health and Care: Scoping Review. *JMIR Mhealth Uhealth*. Jul 13 2022;10(7):e35684. doi:10.2196/35684
5. Kreitmair KV. Mobile health technology and empowerment. *Bioethics*. Jul 2024;38(6):481-490. doi:10.1111/bioe.13157
6. Esmaeili B, Vieluf S, Dworetzky BA, Reinsberger C. The Potential of Wearable Devices and Mobile Health Applications in the Evaluation and Treatment of Epilepsy. *Neurol Clin*. Nov 2022;40(4):729-739. doi:10.1016/j.ncl.2022.03.005

7. Hansen C, Sanchez-Ferro A, Maetzler W. How Mobile Health Technology and Electronic Health Records Will Change Care of Patients with Parkinson's Disease. *J Parkinsons Dis*. 2018;8(s1):S41-s45. doi:10.3233/jpd-181498
8. Gyselaers W, Lanssens D, Perry H, Khalil A. Mobile Health Applications for Prenatal Assessment and Monitoring. *Curr Pharm Des*. 2019;25(5):615-623. doi:10.2174/1381612825666190320140659
9. Rabinovich L, Molton JS, Ooi WT, Paton NI, Batra S, Yoong J. Perceptions and Acceptability of Digital Interventions Among Tuberculosis Patients in Cambodia: Qualitative Study of Video-Based Directly Observed Therapy. *J Med Internet Res*. Jul 27 2020;22(7):e16856. doi:10.2196/16856
10. Yuan NP, Brooks AJ, Burke MK, et al. My Wellness Coach: evaluation of a mobile app designed to promote integrative health among underserved populations. *Transl Behav Med*. Jul 7 2022;12(6):752-760. doi:10.1093/tbm/ibac015
11. Zheng YL, Ding XR, Poon CC, et al. Unobtrusive sensing and wearable devices for health informatics. *IEEE Trans Biomed Eng*. May 2014;61(5):1538-54. doi:10.1109/tbme.2014.2309951
12. Yetisen AK, Martinez-Hurtado JL, Ünal B, Khademhosseini A, Butt H. Wearables in Medicine. *Adv Mater*. Jun 11 2018;30(33):e1706910. doi:10.1002/adma.201706910
13. Khatiwada P, Yang B, Lin JC, Blobel B. Patient-Generated Health Data (PGHD): Understanding, Requirements, Challenges, and Existing Techniques for Data Security and Privacy. *J Pers Med*. Mar 3 2024;14(3)doi:10.3390/jpm14030282
14. Wen D, Zhang X, Lei J. Consumers' perceived attitudes to wearable devices in health monitoring in China: A survey study. *Comput Methods Programs Biomed*. Mar 2017;140:131-137. doi:10.1016/j.cmpb.2016.12.009
15. Seneviratne S, Hu Y, Nguyen T, et al. A Survey of Wearable Devices and Challenges. *IEEE Communications Surveys & Tutorials*. 2017;19:2573-2620.
16. Filkins BL, Kim JY, Roberts B, et al. Privacy and security in the era of digital health: what should translational researchers know and do about it? *Am J Transl Res*. 2016;8(3):1560-80.
17. Silva-Trujillo AG, González González MJ, Rocha Pérez LP, García Villalba LJ. Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack. *Sensors (Basel)*. Jun 8 2023;23(12)doi:10.3390/s23125438
18. Cuningkin V, Riley E, Rainey L. Preventing Medjacking. *Am J Nurs*. Oct 1 2021;121(10):46-50. doi:10.1097/01.NAJ.0000794252.99183.5e
19. Cilliers L. Wearable devices in healthcare: Privacy and information security issues. *Health Inf Manag*. May-Sep 2020;49(2-3):150-156. doi:10.1177/1833358319851684
20. Statista. Annual number of data compromises and individuals impacted in the United States from 2005 to 2023. Statista. Accessed August 12, 2024. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
21. Huckvale K, Prieto JT, Tilney M, Benghozi PJ, Car J. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *BMC Med*. Sep 7 2015;13:214. doi:10.1186/s12916-015-0444-y
22. Mukhopadhyay A. How India's loose data privacy laws open the door to hackers. DW. Accessed August 8, 2024. https://www.dw.com/en/how-indias-loose-data-privacy-laws-open-the-door-to-hackers/a-53120972
23. Els F, Cilliers L. Improving the information security of personal electronic health records to protect a patient's health information. *2017 Conference on Information Communication Technology and Society (ICTAS)*. 2017:1-6.
24. Perez-Pena R, Rosenberg M. Strava Fitness App Can Reveal Military Sites, Analysts Say. *The New York Times*. January 29, 2018. https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html
25. Heidel A, Hagist C, Schlereth C. Pricing through health apps generated data-Digital dividend as a game changer: Discrete choice experiment. *PLoS One*. 2021;16(7):e0254786. doi:10.1371/journal.pone.0254786
26. Rising CJ, Gaysynsky A, Blake KD, Jensen RE, Oh A. Willingness to Share Data From Wearable Health and Activity Trackers: Analysis of the 2019 Health Information National Trends Survey Data. *JMIR Mhealth Uhealth*. Dec 13 2021;9(12):e29190. doi:10.2196/29190
27. The Lancet Digital H. Wearable health data privacy. *Lancet Digit Health*. Apr 2023;5(4):e174. doi:10.1016/s2589-7500(23)00055-9
28. Segura Anaya LH, Alsadoon A, Costadopoulos N, Prasad PWC. Ethical Implications of User Perceptions of Wearable Devices. *Sci Eng Ethics*. Feb 2018;24(1):1-28. doi:10.1007/s11948-017-9872-8
29. Hart K. Genetic testing firms share your DNA data more than you think. Axios. Accessed October 27, 2022. https://www.axios.com/2019/02/25/dna-test-results-privacy-genetic-data-sharing
30. Schreiber R, Koppel R, Kaplan B. What Do We Mean by Sharing of Patient Data? DaSH - A Data Sharing Hierarchy of Privacy and Ethical Challenges. *Appl Clin Inform*. Jul 25 2024;doi:10.1055/a-2373-3291
31. Liddell K, Simon DA, Lucassen A. Patient data ownership: who owns your health? *J Law Biosci*. Jul-Dec 2021;8(2):lsab023. doi:10.1093/jlb/lsab023
32. Sharma R. Who really owns your health data? Forbes. Accessed August 13, 2024. https://www.forbes.com/sites/forbestechcouncil/2018/04/23/who-really-owns-your-health-data

33. Royal K. Who owns patient medical records? Journal of Urgent Care Medicine. Accessed August 13, 2024. https://www.jucm.com/owns-patient-medical-records/
34. DOT Security. Who owns the data collected by wearable devices? DOT Security. Accessed August 13, 2024. https://dotsecurity.com/insights/blog-who-owns-data-collected-by-wearable-devices
35. Austin P. The real reason Google is buying Fitbit. Time. Accessed August 13, 2024. https://time.com/5717726/google-fitbit/
36. Acosta JN, Falcone GJ, Rajpurkar P, Topol EJ. Multimodal biomedical AI. *Nat Med*. Sep 2022;28(9):1773-1784. doi:10.1038/s41591-022-01981-2
37. Khalid N, Qayyum A, Bilal M, Al-Fuqaha A, Qadir J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Comput Biol Med*. May 2023;158:106848. doi:10.1016/j.compbiomed.2023.106848
38. Siontis KC, Noseworthy PA, Attia ZI, Friedman PA. Artificial intelligence-enhanced electrocardiography in cardiovascular disease management. *Nature Reviews Cardiology*. 2021/07/01 2021;18(7):465-478. doi:10.1038/s41569-020-00503-2
39. Seh AH, Zarour M, Alenezi M, et al. Healthcare Data Breaches: Insights and Implications. *Healthcare*. 2020;8(2). doi:10.3390/healthcare8020133
40. Attia ZI, Harmon DM, Behr ER, Friedman PA. Application of artificial intelligence to the electrocardiogram. *Eur Heart J*. Dec 7 2021;42(46):4717-4730. doi:10.1093/eurheartj/ehab649
41. van den Beuken WMF, van Schuppen H, Demirtas D, et al. Investigating Users' Attitudes Toward Automated Smartwatch Cardiac Arrest Detection: Cross-Sectional Survey Study. *JMIR Hum Factors*. Jul 25 2024;11:e57574. doi:10.2196/57574
42. Hindelang M, Wecker H, Biedermann T, Zink A. Continuously monitoring the human machine? - A cross-sectional study to assess the acceptance of wearables in Germany. *Health Informatics J*. Apr-Jun 2024;30(2):14604582241260607. doi:10.1177/14604582241260607
43. Devine JK, Schwartz LP, Hursh SR. Technical, Regulatory, Economic, and Trust Issues Preventing Successful Integration of Sensors into the Mainstream Consumer Wearables Market. *Sensors (Basel)*. Apr 2 2022;22(7)doi:10.3390/s22072731
44. Dobson R, Stowell M, Warren J, et al. Use of Consumer Wearables in Health Research: Issues and Considerations. *J Med Internet Res*. Nov 21 2023;25:e52444. doi:10.2196/52444
45. The American Medical Association. Patient perspectives around data privacy. The American Medical Association,. Accessed August 7, 2024. https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf
46. Chikwetu L, Miao Y, Woldetensae MK, Bell D, Goldenholz DM, Dunn J. Does deidentification of data from wearable devices give us a false sense of security? A systematic review. *Lancet Digit Health*. Apr 2023;5(4):e239-e247. doi:10.1016/s2589-7500(22)00234-5
47. Yeke D, Ibrahim M, Tuncay GS, et al. Wear's my data? Understanding the cross-device runtime permission model in wearables. Google Research. Accessed August 12, 2024. https://research.google/pubs/wears-my-data-understanding-the-cross-device-runtime-permission-model-in-wearables/
48. Li Z, Wang B, Li J, Hua Y, S Z. Local differential privacy protection for wearable device data. *PLoS ONE*. 2022;17(8):e0272766. doi:19.137/journal.pone.0272766
49. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*. Jul 2018;113:48-52. doi:10.1016/j.maturitas.2018.04.008
50. El-Tallawy SN, Pergolizzi JV, Vasiliu-Feltes I, Ahmed RS, LeQuang JK, Alzahrani T, Varrassi G, Awaleh FI, Alsubaie AT, Nagiub MS. Innovative Applications of Telemedicine and Other Digital Health Solutions in Pain Management: A Literature Review. Pain Ther. 2024 Aug;13(4):791-812. doi: 10.1007/s40122-024-00620-7.
51. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare Challenges in the Era of Cybersecurity. *Health Secur*. May/Jun 2020;18(3):228-231. doi:10.1089/hs.2019.0123