Your Data, Their Rules: Digital Health Privacy in the UK and EU

Authors: Shohrah Kadwani, Swati Dahiya, Shivangi Bhupendra, Krishnapriya K S, Archit Bhattacharya and Ayeni Sarah Biola

International Institute of SDGS & Public Policy Research

Abstract

The rapid expansion of digital health technologies through wearable devices, health applications, and AI-driven technologies has created a shift in how traditional patient health data is being handled. As health data increasingly shifts from traditional healthcare institutions to consumer-facing digital platforms, it creates regulatory challenges that existing legal frameworks were not designed to address. This paper examines how effectively the United Kingdom and European Union protect digital health data privacy in this evolving environment. This paper uses a qualitative and comparative approach to analyse the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025, the European Union's General Data Protection Regulation (GDPR), and the European Health Data Space (EHDS). Research was conducted into legislation, academic literature and case studies, and the paper is divided into three interconnected themes: wearable technologies, public trust and consent. The findings draw on the concept of regulatory lag, and suggest that despite comprehensive legal frameworks, both jurisdictions face a common structural problem: technological innovation seems to be advancing faster than policy can respond. Wearable technologies blur the distinction between lifestyle and health data to exploit the gaps in existing regulatory frameworks, and current consent mechanisms often fail to provide meaningful user control over data. This paper argues that both the UK and EU have largely adopted a reactive, rather than a proactive approach to digital health governance and emphasises a need to incorporate stronger consent mechanisms, oversight of wearable technologies and clearer accountability structures to adapt to an increasingly digital healthcare environment.

1. Introduction

Throughout much of modern medical history, medical records and sensitive health data existed within traditional healthcare institutions. Rules and regulations on the use, collection and access of health data were relatively clear, with clear roles for actors such as doctors, hospitals, and healthcare administrators. If something went wrong, it was clear who was responsible - the doctor, the hospital, the staff that worked that day. This data is now referred to as traditional healthcare data. The rapid growth of digital health technology has fundamentally altered this model, creating challenges that existing healthcare regulations were not designed to address (Zulueta, 2021). Today, smartwatches, fitness trackers, and AI wearable devices generate and collect thousands of data points of information relating to heart rate, sleep patterns, physical activity, menstrual cycles, stress levels, and other indicators of health and well-being (Doherty et al., 2025). This digital health data is also called “lifestyle data” due to its intimate nature and also due to the fact that it is passively collected, often not fully understood by users. (Takka, 2023). The introduction of this kind of big data does not come without its ethical, legal and political consequences. As data has become an invaluable resource, the shift from traditional, institution-monitored, legally protected data to corporation-held, commercially driven, and legally ambiguous data is one of the most significant regulatory challenges faced by contemporary health systems (Takka,2023). This paper aims to examine the functioning and performance of existing protections against the risks of data privacy created by apps, wearables, and AI technologies in the EU and the UK. This paper examines digital health data privacy through three key themes: consent, wearable technologies, and public trust. Despite the existence of data protection legislation in both countries (Zulueta,2021), structural gaps in policy, loopholes in the system, consent mechanisms and weak regulation and enforcement portray a bleak picture. Policies seem to, unfortunately, fall behind when compared to the rate at which AI technology and data collection have adapted (Doherty et al., 2025)

Before we continue, it is important to clarify the jurisdictions that are under comparison. After Brexit in 2021, the United Kingdom developed its own unified legal framework governing digital health data. First, the UK General Data Protection Regulation, which was retained from EU law, following Brexit. Second, the Data Protection Act 2018. These together (along with the recent Data Use and Access Act 2025) are responsible for establishing the foundational rules on how health data is collected, protected, processed and stored. The functioning of these is overseen by two main regulators: the Information Commissioner's Office, which oversees data protection compliance within the NHS and health apps and the Medicines and Healthcare products Regulatory Agency (MHRA), which regulates the smaller niche of medical devices and AI diagnostic tools. Together, these instruments form a relatively coherent national framework. On the other hand, each of the 27 sovereign member states of the EU have their own legal systems, healthcare infrastructure, and regulatory capacity. When this paper refers to the EU framework, it refers to the overarching legislation set in place, which includes the policies and the rules that set binding standards, but are naturally implemented and enforced differently in each member state. The framework in the EU consists of the General Data Protection Regulation, 2018, and the European Health Data Space Regulation 2025. These combined established a comprehensive framework for both primary and secondary use of health data. It is important to note that there exists a gap between what its legislation requires on paper and how consistently it is applied across 27 states. Hence, the UK and EU in 2026 represent two distinct regulatory policies evolving from the same starting point, not just legally but also institutionally, as many digital health companies and NHS-linked organisations operate across both the UK and EU. This paper asks the question: Do existing UK and EU digital

health privacy frameworks adequately protect individuals in the age of wearable technologies, consent, and public trust? This paper uses a qualitative and comparative approach, drawing on regulations, case studies and secondary data to argue that digital health technology has outpaced the law. As a result, its conclusions are based on existing research rather than primary data. Additionally, this paper draws on the concept of "regulatory lag". Regulatory lag is a term used to describe the tendency of legal frameworks to respond to technological change reactively rather than anticipatorily (Baldwin, Cave & Lodge, 2012). It is also important to note that many EHDS secondary-use provisions do not take effect until 2029, hence this paper critiques its intended design and operation rather than its real-world performance. The first chapter delves into regulations for apps and wearables, and the second chapter analyses consent and public trust mechanisms. Despite their differences, both the UK and EU frameworks share a common and fundamental failure: Laws have been reactive, rather than proactive. This paper calls for stronger, future-proof regulations that should be capable of anticipating the risks of emerging health and data technologies. It also recommends transparent consent and accountability mechanisms within policies, so that individuals retain control over their health data and that organisations collecting such data operate within clear systems of accountability.

2. Literature Review

The literature review covers two sections on interrelated themes: first, consent as a governing mechanism for digital health data, and second, the regulation of wearable and smartphone health technologies in the UK and EU. These themes, together, demonstrate a recurring tension between existing legal frameworks and the pace of digital health innovation.

2.1 Consent and public trust

While existing EU and UK data protection frameworks seek to address data privacy concerns, questions remain regarding their effectiveness in the digital health context. This section of the literature review focuses on the importance of public trust and consent in the digital health data privacy sector. Present studies identify consent as a central challenge in digital health governance. As digital health technologies advance, several scholars have questioned whether traditional models of informed consent remain effective. Existing privacy structures find it difficult to keep pace with digital health innovation, creating uncertainty with regard to meaningful consent practices (Kassam et al.,2023). As health data is being collected and reused on a large scale, the traditional informed consent models are being challenged. While patients are generally willing to share health data, their willingness is highly contingent on transparency regarding who can access their information, its usage and what protection mechanisms are in place to safeguard their privacy. Thus, it can be noted that consent alone may be insufficient unless backed by honest communication and strong governance means.

Current consent mechanisms are often difficult for people to comprehend, thereby raising concerns about whether consent is genuinely informed (Wiertz and Boldt, 2024). In general, patients are willing to share their health information when data users communicate privacy protections clearly (Kassam et al., 2023). However, the complex privacy policies make it impossible for people to understand what they are consenting to. Also, considerable attention has been paid to the fact that patients prefer control over how their data is used and also express apprehension regarding commercial access and international data transfers. A growing body of literature consistently implies that although consent remains imperative to the UK and EU data protection systems, the current mechanism may not effectively address the intricacies of digital health data handling.

Cascini et al. (2024) argue that public support for the secondary use of health data depends on how data is accessed and managed. Their review primarily suggests that, while several individuals acknowledge the potential advantages of data sharing for research and health sector improvement, concerns regarding privacy, security and loss of control are some significant barriers. These findings add to our understanding of the need for transparency and public awareness to strengthen weak links, thereby encouraging more responsible participation in health data sharing. The literature further emphasises the importance of public trust, which is emerging as a key concern within debates surrounding digital health governance. According to Gille, Smith and Mays (2022), public trust is essential for the successful use and sharing of health data within modern health care systems. This reflects an emerging theme throughout the literature, that trust is strengthened through honesty, accountability and public engagement. It is emphasised that trust cannot be maintained through legal actions alone, but requires ongoing communication and tangible protective measures that reassure individuals that their personal information is being handled responsibly. These findings are particularly relevant to the UK and EU, where increasing reliance on digital health technologies has intensified debates around privacy and data governance. The literature, therefore, suggests that both consent and trust are closely interconnected.

2.2 Wearables, apps, and regulatory gaps

The use of wearable technology and smartphone applications in the modern healthcare landscape reflects a significant shift in patient observation and care. The digitally acquired health data apparently captures an individual's behaviour, and factors that impact behavioural change in the moment, and over time (Marsch, 2020). Through the production of consumer-facing health apps and wearable devices, the multi-billion-dollar health tech industry has made a major move into the global healthcare system (Thomason, 2021). The utility of these technologies by individuals generates large sets of data that could be used for both primary (personal) use and secondary care, such as medical research, public health monitoring, and AI-driven healthcare innovations (Dixon, et al. 2023). However, when it comes to the secondary use, there is a need to build mutual trust among the various stakeholders involved in health data governance and to protect individuals from possible threats. This section of the literature review explores the UK and EU regulatory mechanisms regarding wearable devices and mobile applications. Also, it seeks to identify structural gaps in the policies that fail to protect the health data from risks posed by modern technology.

Under the European Union's General Data Protection Regulation (GDPR), user consent is required for processing and sharing of personal data acquired through smartphone applications and wearable technologies (Art. 7 GDPR, 2023). This is supplemented by a harmonised framework for sharing health data across Member States through the European Health Data Space (EHDS) regulation. Working alongside the GDPR, the EHDS seeks to establish mechanisms for secondary use without individual consent (Regulation EU) and integrate self-generated data from apps and wearables with clinical records, thereby making data accessible for patient care and research purposes (Cimina, 2023). Existing literature, however, highlights ambiguity regarding whether wellness app providers would be legally required to transfer health data for secondary use under the EHDS, and if so, how meaningful user control would be ensured (Brückner S. et al 2025). In the United Kingdom, the NHS data supports a global research ecosystem. However, a study has identified multistage fragmented data flows, data interactions that do not fulfil recommended practices for safe data access, and existing infrastructure that produces aggregation of duplicate data assets (Zhang J. et al. 2023). This fragmentation is not a mere technical inefficiency: it directly undermines the transparency that Gille, Smith and Mays (2022) identify as foundational to public trust, linking the regulatory and trust strands of this review.
Further, an observable gap emerges from device classification. Wearable technologies in the UK are largely regulated

based on their proposed intent. Often, wearables are advertised as health devices, but not all fall within the category of medical devices. The first classification of devices as consumer products or devices for medical use is done by the manufacturer. The Medicines and Healthcare products Regulatory Agency (MHRA), then, categorises these medical devices according to their safety risks (UK POSTnote 741). Those regulated as consumer products may face less scrutiny regarding safety, security, and health inequity issues than medical products (Mistry P. et al. 2020). This creates a loophole in the regulatory system where devices capable of generating vital sensitive data may be subjected to lower levels of scrutiny than formally recognised medical devices.

Scholars have frequently raised concerns regarding privacy, transparency, and user autonomy in both jurisdictions. Previous studies conducted in the UK manifested a significant proportion of sensitive user data being shared with third parties by health-tracking applications, which may not comply with the UK GDPR (Privacy International, 2020). The EHDS seeks to create a connected health data ecosystem, where users are required to be aware of what they consent to. But app developers deliberately design complex consent interfaces that undermine people's ability to understand (Brightwell C. et. al. 2024). Consequently, many users remain unaware of when, where and how their health data is shared. Across both themes, the literature converges on a single underlying problem: legal consent requirements in the UK and EU were designed for a slower-moving, more centralised model of data collection and have not kept pace with the scale, fragmentation, and commercial complexity of digital health technologies.

3. Apps and Wearables

The growth of wearable technologies in contemporary times has complicated the question of what legally qualifies as health data (Bouderhem, 2023; Ducato, 2023). This chapter examines the challenges that wearable technologies and AI-driven health systems have posed towards the existing regulatory frameworks in the UK and the EU (Thorogood & Tovino, 2024; Radanliev, 2025). It also argues that the growing convergence of consumer technology and healthcare requires a more adaptive regulatory approach, which is capable of addressing emerging issues related to data classification, privacy, accountability and governance (Thorogood & Tovino, 2024; Radanliev, 2025). A single heart rate may appear insignificant in isolation, but when collected continuously over time, such information has the potential to reveal important insights into an individual's physical or mental health (Ducato, 2023; Radanliev, 2025). In the UK, the MHRA mainly focuses on safety, effectiveness and accuracy rather than privacy (Bouderhem, 2023), leaving millions of products that collect data outside the framework.

The European Health Data Space regulation attempts to create a more robust framework for online digital health governance across the European Union. It has expanded the rules related to health data access, sharing, primary and secondary rules (Thorogood & Tovino, 2024). For example, in 2024, the Finnish Data Protection Ombudsman imposed a fine of more than €120,000 on Oura for processing smart ring users' health related data without obtaining valid consent. The case has illustrated that increasing regulatory attention is given to wearable technologies and the legal challenges surrounding the classification and use of wearable-generated health information. But, still, the uncertainty remains about the wearable information generated outside the formal healthcare system (Ducato, 2023; Bouderhem, 2023). This uncertainty arises because wearable devices often collect biometric information such as heart rate, sleep patterns and activity levels, which fall outside traditional healthcare settings (Ducato, 2023; Radanliev, 2025). As a result, regulators are facing obstacles in determining whether such information should count as ordinary

personal data or as sensitive health data deserving legal protection under the GDPR (Malgieri & Niklas, 2019; Ducato, 2023; Thorogood & Tovino, 2024). The EU attempted enforcement through the Oura fine, but a single fine does not constitute a regulatory framework. Examining ICO enforcement shows that UK consumer wearable data privacy is an unrepresented subject (ICO, 2025). This absence reflects a wider trend of uneven enforcement capability rather than any problem specific to the UK; according to the recent study of the activities of various data protection authorities across Europe comparing them across their enforcement of data protection with respect to AI and device-generated data shows that many compliant regulators are grouped in countries like Italy, Spain, France, Germany, Austria, and the Netherlands while many other authorities are inactive and make no meaningful decisions (Mazur et al., 2026). The UK is not included in this study which covers the EU-27 members meaning the comparison is more illustrative than clarifying the score but even compared to that oppressive model the situation of the Oura fine put Finland's enforcement authority into a much more active tier while the ICO's absence of a similar case puts its authorities into a situation closer to the inert and reluctant enforcers of the EU who cite the lack of resources as the cause of inactivity (Mazur et al., 2026). This fits well into the more extensive scholarship that doubts whether the regulators can be assessed only through counting their enforcement actions (Buckley et al., 2024), a caution that is essential to bear in mind while performing a UK vs EU comparison based on the enforcement data.

The GDPR considers health data mainly as highly sensitive information that requires strong legal protection. However, the use of wearable technologies makes the definition of what health data is difficult (Malgieri & Niklas, 2019; Ducato, 2023). There is an example of how information that may seem like ordinary lifestyle data can be sensitive health information when viewed over time (Ducato, 2023). Similarly, information relating to sleep patterns may appear as ordinary lifestyle data. This demonstrates how data that appears non-medical at first can gradually acquire health significance (Ducato, 2023; Radanliev, 2025). The increasingly blurred distinction between lifestyle information and medical information makes it difficult for existing legal frameworks to provide a clear and consistent boundary between the two (Ducato, 2023; Malgieri & Niklas, 2019). The existing legal frameworks have failed to provide a clear boundary between them. All these reflect how digital health technology transformation has taken place faster than the legal categories used to regulate it; this raised the question at which point wearable health information is considered part of health data (Thorogood & Tovino, 2024; Ducato, 2023). This reflects the concept of regulatory lag, where legal frameworks respond to technological innovation only after new technologies have already transformed existing practices (Baldwin, Cave & Lodge, 2012). The challenge for both the UK and the EU is not the absence of legal protection, but uncertainty regarding when consumer-generated wearable information becomes legally protected health data (Ducato, 2023; Thorogood & Tovino, 2024). What's clear here is that both jurisdictions share the same fundamental problem, but neither has resolved it. The UK, through MHRA, and the EU, through the EHDS, have each attempted to expand their frameworks, yet both continue to rely on classification based on categories. These categories keep expanding as the world advances, and were not designed for continuous and passive data collection.

3.1 Wellness loopholes

Unlike traditional healthcare systems, wearable technologies are largely based on continuous and passive data collection. Smartwatches, fitness trackers, sleep monitors and health applications periodically collect behavioural, biometric and location information during a user's daily life (Bouderhem, 2023; Radanliev, 2025). Instead of relying on conventional healthcare, where information is generally collected during specific clinical interactions, wearable technologies generate ongoing streams of personal data. This change has uncovered a major regulatory gap, commonly referred to as the "wellness loophole" (Bouderhem, 2023). In the UK, many wearable devices and health apps avoid

medical device regulation by marketing themselves as wellness or lifestyle products, rather than as diagnostic or therapeutic products (Bouderhem, 2023). The MHRA's regulatory framework focuses on products that make medical claims or have a medical purpose. As a result, a large number of consumer health apps operate outside the scope of formal medical device regulation, even though they generate information that can potentially give significant insight into an individual's health status (Bouderhem, 2023). This means that products that are capable of generating health-related insights are less regulated simply because of the way they are categorised (Bouderhem, 2023). A device that continuously monitors heart rate and predicts health conditions is treated differently from a clinical device performing the same function, simply because the manufacturer chose to market it as a wellness product. By 2021, almost 100,000 health-related apps existed in the UK market alone, yet only those qualifying as medical devices were required to register with the MHRA (Narain & Lally, 2025). The European Union has attempted to deal with some of these challenges through the European Health Data Space (EHDS), which seeks to improve access to and governance of health-related information across connected digital services within the EU (Thorogood & Tovino, 2024). The EHDS expands the scope of regulations related to health data. However, many consumer-oriented wearable technologies and wellness applications remain disconnected from traditional healthcare systems. As a result, this has created ambiguity about how to classify and regulate information generated through these technologies, particularly when data is being generated in a consumer's hand rather than a clinical context (Thorogood & Tovino, 2024). This is a structural loophole, seemingly easy to take advantage of. It emphasises the need for a clear system of categorisation and classification for health care devices.

The continued existence of this loophole points to broader structural limits in the way regulations are designed in the UK and the EU. The current regulatory frameworks were mainly developed to cover hospitals, healthcare professionals and medical service providers. They assume that health data is generated within the formal healthcare sector and subsequently managed through established institutional processes. Wearable technologies undermine these assumptions by producing health-related information through consumer products outside the formal healthcare setting (Bouderhem, 2023; Ducato, 2023). This makes it harder for regulatory systems to determine when wellness data becomes health data and when consumer technologies need to be subjected to a more stringent regulatory regime (Thorogood & Tovino, 2024). This reflects the concept of regulatory lag, where regulatory frameworks struggle to keep pace with technological innovation and continue to rely on assumptions that no longer reflect how health data is generated (Baldwin, Cave & Lodge, 2012).

3.2 AI and new risks

The increasing use of artificial intelligence in wearable technologies has resulted in a new set of challenges for the governance of health data. Earlier, wearables mainly focused on the collection of information such as heart rate or sleep patterns. But this has changed with the coming of AI into wearables. Modern AI wearables have gone beyond simple data collection to the generation of predictions and recommendations from the information gathered by the users (Radanliev, 2025). This has created new concerns because wearable technologies are no longer simply reading existing health information. Instead, they have moved into new health information generation through the predictions and inferences made (Radanliev, 2025). For example, AI may identify patterns associated with a disorder for someone having a certain type of sleep pattern. This creates a problem when it is done without the consent of the user (Radanliev, 2025). As a result, the distinction between collected data and

generated health information is getting harder to identify (Ducato, 2023; Radanliev, 2025). Another concern relates to the "black box" nature of many AI technologies. There isn't a follow-up on how and why a particular recommendation or prediction was made. There is no mention of the base that was used. This suggests that the lack of an explanatory mechanism erodes trust in AI-based tech, especially when individuals increasingly rely on these devices to make decisions concerning their health and well-being (Radanliev, 2025). The limited transparency also reduces user autonomy because individuals may follow AI-generated recommendations with a naive understanding of the reasoning behind that decision (Radanliev, 2025). Research into secondary sources tells a bleak story; the ICO and EU AI Act both recognise and acknowledge the risks of using AI health tools, yet in both cases, acknowledgement has not translated into enforceable, specific regulation of AI-generated inferences from wearable data.

The use of AI has created accountability concerns as well. When an AI tech produces an inaccurate or missing health insight, it becomes difficult to determine who should be responsible. Responsibility may be shared between device manufacturers, software developers and data processors as there is no clear department taking responsibility. This creates ambiguity about who should be held responsible (Radanliev, 2025). Both the UK and EU have taken steps to create rules governing the collection, storage and processing of health information. However, they lag in terms of the regulation of AI-generated health predictions. This reflects how existing regulatory frameworks face growing difficulties in addressing explainability, accountability, trust, and user autonomy within digital health (Radanliev, 2025; Thorogood & Tovino, 2024). The proliferation of digital health technologies has exposed significant gaps in the current policy frameworks of both countries. Both the UK and the EU, reacting to this resultant crisis, have taken new measures to strengthen health data protection, improve regulatory oversight and respond to the growing role of digital technologies in healthcare (Thorogood & Tovino, 2024). Nevertheless, significant challenges remain regarding the consumer-generated health information, wearable technologies and AI-driven health systems (Bouderhem, 2023; Radanliev, 2025; Thorogood & Tovino, 2024). Therefore, regulation has to be proactive, addressing the problem continuously as well as predictively.

Most existing regulatory frameworks were developed around hospitals, healthcare professionals, insurers and recognised medical devices. Modern digital health ecosystems operate very differently. Health information is increasingly generated through wearable devices, mobile applications, AI systems, telehealth platforms and cloud-based services that often exist outside traditional healthcare environments (Bouderhem, 2023; Radanliev, 2025). Although the UK and EU have adopted different regulatory approaches, they continue to face the same underlying challenges. Digital health technologies are evolving faster than legal frameworks, illustrating the concept of regulatory lag. The result is a persistent gap between the protections promised by regulation and the realities of contemporary app-based, wearable and AI-driven health data collection (Thorogood & Tovino, 2024; Ducato, 2023). Regulatory approaches should therefore be forward-looking and flexible rather than reacting to technological developments after the risks have materialised (Thorogood & Tovino, 2024; Radanliev, 2025). Future governance should go beyond the protection of health information once it is collected and anticipate emerging risks associated with wearable technologies, consumer health applications and AI-generated health insights (Radanliev, 2025;Thorogood & Tovino, 2024).

4. Consent mechanisms

As apps, wearables, and AI systems collect increasing amounts of sensitive health information, the question shifts from what data is collected to whether individuals genuinely understand and control how this data collected is used. Consent is the ability of citizens to have total control over their most sensitive personal information. However, in the digital health technology world, this has become just a stepping stone to be passed on the way to the final destination. It is a legal fiction rather than a real power of autonomy for the patients. This chapter argues that the EU and UK have failed to hold meaningful consent for patients, as the health data system was traditionally designed for identifiable institutions to hold data for specific purposes. But the digitisation of healthcare through the use of wearable apps and technologies has now completely changed the system, and the law has not caught up yet. This chapter tackles this failure in two related ways. First, by analysing whether the legal frameworks of the UK and EU create genuinely meaningful consent, and second, by exploring how this failure translates into a broader erosion of public trust through key case studies.

4.1 The Framework of the UK

The UK has a two-tier system. Health data is a special category of data for which explicit consent is required under Article 9 of the UK GDPR. However, the ICO recommends that NHS bodies do not rely on consent as their main lawful basis, as consent in a healthcare setting cannot be “freely given” in the sense of the GDPR; patients in a dependent relationship with their provider have no real choice (Data Protection Act 2018; UK GDPR). The second track, the Common Law Duty of Confidentiality, relies on implied consent for direct care, but falls apart entirely when data moves from clinical purposes to research or commercial use. Another layer is added by the Data (Use and Access) Act 2025 (DUAA) which allows for 'broad consent' under Section 68, whereby patients can give consent to an area of scientific research without being informed of the research purposes in advance (DUAA 2025, s. 68). This is practical for long-term research, but what it does is lower the legal standard of what counts as valid consent. It’s this big, undefined thing that patients sign up for, rather than something they can meaningfully evaluate. The result is a framework that has progressively moved away from genuine patient control. First, by discouraging reliance on consent for NHS processing, and then by introducing broad consent that asks patients to agree to terms that they do not know.

4.2 The Framework of the EU

The EU baseline is similar. GDPR Article 9 requires explicit consent for health data, with a research exception under Article 89 allowing broad consent where consistent with ethics standards (Regulation (EU) 2016/679). The EHDS Regulation 2025/327 is the big difference. The secondary use of health data is available by default, and rather than opting in, patients have the right to opt out (Regulation (EU) 2025/327, Art. 71). This is a very basic philosophical change. The system presumes you are allowed to do something, and you have to say no. There are institutional safeguards, but they are about what happens to data after it is accessed; they do not give patients meaningful control over whether their data even enters the system. While comparing the two frameworks, the direction is similar even if the mechanisms differ. The UK lowers the threshold for valid consent, and the EU effectively removes the consent requirement for secondary use. Both represent a shift in whose interests the framework is designed to serve, and in both cases, the patient is not the answer.

4.3 Failure of Both Systems

In either framework, two structural problems make informed consent meaningless. The first is power imbalance and information asymmetry. For consent to be genuine, the patient must understand what they are agreeing to and have full power to say no without requiring many reasons from their side. Health Data law is spread across multiple overlapping statutes and regulatory bodies. The UK alone operates under GDPR, the common law duty of confidentiality, and now the DUAA 2025, alongside. No patient, no matter how aware they are, can realistically navigate through this. Research consistently shows that public awareness of how health data is used is very low, even among the people who preach on the principle of data sharing (Kerasidou & Kerasidou, 2023; Baines et al., 2024). A consent process that is legally valid but practically unfathomable by the ordinary public is not protecting patients; it is protecting the money-making institutions. The power imbalance makes this more difficult. On one hand, the GDPR requires the public to give their consent freely, whereas on the other hand, the patients who depend on the NHS cannot genuinely refuse. The ICO acknowledges this, which is why it tells the NHS not to rely on consent as a lawful basis, but in reality, this changes nothing. The result is that data processing is moved to bases where it doesn't require active consent from patients. This doesn't remove the problem; it just hides it from view. The second is the opt-out paradox. Both the UK's National Data Opt-out and the EHDS article 71 secondary use opt-out place the burden of denial on the patient rather than on the institutions. An opt-out option only works when the patients are aware that they have this option, they are aware of the reason why they are opting out, and trust the system enough to act (Baines et al., 2024). The UK's own record shows how rarely these kinds of conditions exist. When GDPR launched in 2021, 1.3 million people opted out within a single month, not because they were against research, but because trust was never repaired after care.data collapsed (Redhead et al., 2025). The opt-out existed on paper, but the conditions required to make it happen didn't. The EHDS repeats this at a European level, where uneven national implementation makes Article 71 even harder to exist consistently. Both frameworks have confused having an opt-out option with having genuine consent. They both are not the same thing. The consequences of weak consent extend beyond legal compliance. When individuals feel they lack meaningful control over their data, confidence in digital health systems declines, making public trust a central governance challenge.

4.4 Public Trust and Case Studies

Public trust can be defined as the belief that a person, institution, organisation, or system will act in accordance with expectations of positive and reliable behaviour (OECD, 2022). It plays a key role in digital health governance and acts as a structural requirement. People strongly hold negative sentiments when companies are opaque and insensitive to their personal data (OECD, 2022), and the repetition of controversies in the digital health sector is a growing problem. These controversies emphasise the need for transparency in consent and accountability mechanisms in policy.

One of the best examples of governance failure is care.data by the NHS (Sterckx et al., 2016). It was initiated in 2013 and ended in 2016 due to controversies faced due to its silence when it came to questions about data management. This project was set to integrate hospital records into a centralised database for planning and research, but the system faced heavy opposition from the public due to inadequate public information strategies. The communication through leaflets and digital notices was not transparent or adequate for the public's under-

standing. An opt-out mechanism is a system in which individuals are automatically included in data collection or processing unless they actively choose to withdraw or refuse participation (Caldicott, 2016; Regulation (EU) 2025/327). The opt-out mechanism is also widely criticised due to its features being misleading and difficult to process (Caldicott, 2016; Sterckx et al., 2016). Similar challenges emerged with the initiation of GPDPR in 2021; the program was about the large-scale extraction of primary care data records. This triggered patients, healthcare professionals, the public, as well as professional bodies like the British Medical Association. Many people falsely believe that they have opted-out (NHS Digital, 2022; Institute for Government, 2023). Due to controversies, the government paused this project in July 2021. This revealed something the UK government had not anticipated: that public trust, once lost through care.data, does not automatically return when a new programme is launched. The 1.3 million opt-outs were an indicator that patients generally reject a system when they believe their data is not being handled responsibly. (Redhead et al., 2025). The Google DeepMind case of 2015-2017 was a reminder that public trust is essential for the deployment of successful projects when sensitive personal health data is involved. The case criticised questions regarding the commercial involvement of the NHS data. The Royal Free NHS Foundation Trust shared approximately 1.6 million patient data points with Google DeepMind to develop the 'Streams' clinical applications to detect acute kidney injury, with no patient consent or involvement. In 2017, the Information Commissioner's Office (ICO) ruled that the trust had breached data protection laws, but no penalties were imposed. The ruling also established that technical legality is insufficient if public expectations and transparency are neglected (Information Commissioner's Office, 2017; Kerasidou & Kerasidou, 2023). The absence of any financial penalty in the Deepmind case and the limited reach of the Oura fine further suggests that breaching health data law carries no meaningful consequences. This enforcement gap exists in both the UK and the EU, where regulatory bodies have the power to fine but frequently choose not to. The data protection law has yet to function as a genuine deterrent in the digital health context.

The lack of punitive fines in the DeepMind case, as well as the limited application of the Oura fine demonstrate inconsistent rather than non-existent enforcement. According to the global statistics on the health sector's external environment, fines in Europe have already led to a total of 265 penalties as well as €32.3 million in total revenue (282% increase from the previous period), alongside the fact that the most notorious violations, such as DeepMind's, have not been subject to financial sanctions. The inconsistency can also be proven by the empirical research showing that some law enforcement agencies in Europe are classified as "inactive" as they have not issued any decisions related to data collection in the healthcare sector (Mazur et al., 2026). The described inconsistency is an example of the deep measurement issue observed by Buckley et al. (2024), who state that the efficiency of privacy regulators cannot be measured easily.

Another major controversy was with Palantir Technologies, a US-based software company, founded in 2003, that focuses on data analytics, Artificial Intelligence, and so on. The controversy began when concerns over trust continued with the NHS Federal Data Platform (FDP) operated by Palantir. Critics have argued that giving a private US technology company a major role in the NHS data structure creates public trust issues and a greater threat to confidentiality. Many patients were not informed about how their data was being processed. Some critics also argue that Palantir's history with US intelligence agencies, military and immigration poses a potential risk to the UK and its people. Further concerns arose in 2026, when reports suggested that the data was

available to non-NHS contractors before pseudonymisation. The FDP debate demonstrates how concerns about transparency, commercial influence, and accountability continue to shape public trust in digital healthcare systems (NHS England, 2023; Medact, 2026; Smith et al., 2026). The Palantir controversy is the most significant of the four case studies because it is ongoing and unresolved. Unlike care.data or GPDPR, which were scrapped in response to public pressure, the Palantir issue has continued despite sustained opposition. This suggests that the UK's governance model has become less responsive to public trust concerns over time, not more. At the European level, a similar situation exists with the European Health Data Space (EHDS). The EHDS aims to create a framework for sharing healthcare data across EU member states for research, innovation, and public health purposes. They are also responsible for sharing cross-border data for the above-mentioned purposes. Concerns have also been raised about the anonymisation and the lack of consistent opt-out rights across member states. While the EHDS seeks to promote innovation, many questions remain about whether citizens will feel confident that their data is being used fairly and responsibly (van Drumpt et al., 2025; Taylor Wessing, 2025). Data access and research innovation have been prioritised over patient control, and public trust has suffered as a result. The difference is that the UK's trust failures are documented and ongoing, while the EUs are anticipated but not yet fully materialised. The EHDS has the opportunity to learn from the UK's mistakes.

In both frameworks, the case studies and public sentiments consistently demonstrate that consent is a legal gateway, not actual protection. The DUAA lowers the bar for valid consent dramatically, while the EHDS effectively eliminates it for secondary use. Neither was built for a world where continuous, passive, commercially run digital health data collection is the norm. This structural failure is not abstract but plays out in real governance crises. Time and again, health data initiatives have foundered because institutions have treated trust as a communications issue rather than a fundamental aspect of governance itself. It is clear in the data of the cases of care.data, GPDPR, Google DeepMind and the Palantir-NHS FDP: when patients feel they haven't really consented to what happens to their data, the whole system of trust collapses. Being legal doesn't necessarily mean you're legitimate. Transparency, robust opt-out mechanisms and authentic public participation are not optional add-ons to good governance. They are its foundation. This chapter additionally demonstrated the need for transparency and options for opt-out as a key to gaining public trust. The success of digital health care policies and initiatives that include sensitive patient data depends highly on public trust. Legal compliance alone is not enough to guarantee legitimacy. Repeatedly, health data initiatives have struggled because institutions treated trust as a communication problem rather than a core part of governance itself.

5. Conclusion and Reccomendations

This paper aims to examine the effectiveness of UK and EU digital health privacy frameworks in light of modern technological challenges, including wearable technologies, consent, and public trust. It uses regulatory lag, the reactive nature of legal frameworks in response to technological changes rather than anticipatorily (Baldwin, Cave & Lodge, 2012), as its core concept used in analysis. The answer that surfaced is that both the EU and the UK digital health frameworks fail in addressing modern issues. The system that was designed to regulate healthcare became oriented toward consumer devices and platforms, and not toward institutional environments. The data that was originally produced and analysed by clinicians is now classified as ordinary "lifestyle data," which is not governed by frameworks that were developed for this purpose. Takka (2023) and Doherty et al. (2025) state that it

is possible to talk about policy lagging behind technological advancement, and this problem can be seen in the degradation of consent. Patient autonomy used to depend on consent, but recently it has become nothing more than a formality. The DUAA reduces the bar of acceptable valid consent, while the EHDS removes the consent requirement completely for secondary use. Most of the time, patients still don't know how their data is being accessed or by whom.

The same pattern shows up in wearable technology governance. Both the UK and the EU are working from the same underlying problem, and neither has really solved it. The MHRA and the EHDS have each expanded their frameworks over time, but both still sort devices into fixed categories instead of looking at what they actually do with consumer data. Devices capable of generating genuinely health-significant insights are routinely marketed as wellness products instead of medical devices, which keeps them outside the reach of existing regulation simply because of how they've been labelled (Bouderhem, 2023). Public trust has taken a hit. Time and again, failures like care. data, GPDPR, the Google DeepMind case, and the still-unfolding Palantir NHS FDP controversy get treated as Public Relations scandals rather than what they really are: structural failures. Palantir is the clearest sign of where things actually stand. Care.data and GDPR both got shelved once public pushback built up, but Palantir has kept going despite that same kind of resistance. That difference says a lot: it suggests the UK's approach to governance has become less responsive to public trust over time, not more. Closing this gap will take a unified regulatory standard, one that classifies devices by what they actually collect and do rather than how manufacturers choose to market them. Regulation also needs to become genuinely anticipatory. As AI wearables shift from simply recording data to generating predictive health inferences, frameworks need to get ahead of these risks instead of catching up after harm has already occurred.

Genuine patient autonomy doesn't mean much without institutional backing. Consent shouldn't be something patients sign once and can never revisit. Dynamic consent models, which let patients change or withdraw their consent whenever they want, would go a long way toward fixing how static current mechanisms are (Lee et al., 2023). Consent forms and privacy policies also need to be written in plain language that people can actually understand, not the dense legal text most patients have no real hope of parsing. This matters just as much for trust: when patients don't understand what they're agreeing to, trust breaks down, and institutions have too often treated transparency as optional rather than something governance actually requires.

Enforcement is crucial for sustainability. The UK and EU both need independent bodies that can actually identify and penalise breaches of health data protection, free from political and commercial pressure, with penalties that match the severity of the breach, no matter how big or well-established the offender is. The DeepMind ruling is a good example of why this matters: it found a clear breach of data protection law, and still, no penalty followed. That sends a message that violations don't really carry consequences. Every actor handling patient data, whether it's a tech company, an NHS trust, or a private contractor, needs to be held to the same standard. Accountability isn't just a box to tick. It's what actually keeps patient rights protected in practice.

References

Baines, R., Stevens, S., Austin, D., Anil, K., Bradwell, H., Cooper, L., Maramba, I. D., Chatterjee, A., & Leigh, S. (2024). Patient and public willingness to share personal health data for third-party or secondary uses: Systematic review. Journal of Medical Internet Research, 26, Article e50421. https://doi.org/10.2196/50421

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation: Theory, strategy, and practice (2nd ed.). Oxford University Press. https://global.oup.com/academic/product/understanding-regulation-9780199576098

Barn, G. (2025). Consent and its discontents: The case of UK Biobank. Medicine, Health Care and Philosophy. Advance online publication. https://doi.org/10.1007/s11019-025-10276-5

Bouderhem, R. (2023). Privacy and regulatory issues in wearable health technology. Engineering Proceedings, 58(1), Article 87. https://doi.org/10.3390/engproc2023058087

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? Journal of Cybersecurity, 10(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

Brightwell, C., Brückner, S., Halpern, O., & Gilbert, S. (2024). Trust and inclusion in digital health: The need to transform consent. Digital Society, 3, Article 52. https://doi.org/10.1007/s44206-024-00052-0

Brückner, S., Dridi, A., Deshmukh, A., Brightwell, C., Halpern, O., & Gilbert, S. (2025). A user-driven consent platform for health data sharing in digital health applications. npj Digital Medicine, 8, Article 699. https://doi.org/10.1038/s41746-025-02147-3

Caldicott, F. (2016). Review of data security, consent and opt-outs. National Data Guardian, Department of Health. https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

Cascini, F., Pantovic, A., Puleo, V., Di Maio, L., Ricciardi, W., & Al-Ajlouni, Y. A. (2024). Health data sharing attitudes towards primary and secondary use of data: A systematic review. eClinicalMedicine, 70, Article 102551. https://doi.org/10.1016/j.eclinm.2024.102551

Cervera de la Cruz, P., Lalova-Spinks, T., & Shabani, M. (2026). The European Health Data Space: An opportunity to strengthen citizen rights and engage citizens in health data governance. Frontiers in Medicine, 12, Article 1699941. https://doi.org/10.3389/fmed.2025.1699941

Data Protection Act 2018, c. 12 (UK). https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Data (Use and Access) Act 2025, c. 15 (UK). https://www.legislation.gov.uk/ukpga/2025/15/contents/enacted

Dixon, W. G., van der Veer, S. N., Ali, S. M., Laidlaw, L., Dobson, R. J. B., Sudlow, C., Chico, T., MacArthur, J. A

L., & Doherty, A. (2023). Charting a course for smartphones and wearables to transform population health research. Journal of Medical Internet Research, 25, Article e42449. https://doi.org/10.2196/42449

Doherty, C., Baldwin, M., Lambe, R., Altini, M., & Caulfield, B. (2025). Privacy in consumer wearable technologies: A living systematic analysis of data policies across leading manufacturers. npj Digital Medicine, 8(1), Article 363. https://doi.org/10.1038/s41746-025-01757-1

Ducato, R. (2023). A deep dive into dynamic data flows, wearable devices, and the concept of health data. International Data Privacy Law, 13(2), 124–140. https://doi.org/10.1093/idpl/ipad007

Gille, F., Smith, S., & Mays, N. (2022). Evidence-based guiding principles to build public trust in personal data use in health systems. Digital Health, 8, 1–11. https://doi.org/10.1177/20552076221111947

GDPR Enforcement Tracker Report 2026: Life Science & Healthcare. (2026). CMS Law. https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/life-science-healthcare

Information Commissioner's Office. (2017, July 3). Royal Free – Google DeepMind trial failed to comply with data protection law [Press release]. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

Kassam, I., Ilkina, D., Kemp, J., Roble, H., Carter-Langford, A., & Shen, N. (2023). Patient perspectives and preferences for consent in the digital health context: State-of-the-art literature review. Journal of Medical Internet Research, 25, Article e42507. https://doi.org/10.2196/42507

Kerasidou, A., & Kerasidou, C. X. (2023). Data-driven research and healthcare: Public trust, data governance and the NHS. BMC Medical Ethics, 24(1), Article 51. https://doi.org/10.1186/s12910-023-00922-z

Lee, A. R., Koo, D., Kim, I. K., Lee, E., Kim, H. H., Yoo, S., Kim, J. H., Choi, E. K., & Lee, H. Y. (2023). Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: A scoping review. BMC Medical Ethics, 24, Article 107. https://doi.org/10.1186/s12910-023-00988-9

Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. Information & Communications Technology Law, 29(2), 197–214. https://doi.org/10.1080/13600834.2019.1643836

Marsch, L. A. (2021). Digital health data-driven approaches to understand human behavior. Neuropsychopharmacology, 46, 191–196. https://doi.org/10.1038/s41386-020-0761-5

Mazur, J., Novelli, C., & Choińska, Z. (2026). Should data protection authorities enforce the AI Act? Lessons from EU-wide enforcement data. International Data Privacy Law, 16(1), ipaf033. https://doi.org/10.1093/idpl/ipaf033

Mistry, P. (2020). The digital revolution: Eight technologies that will change health and care. The King's Fund.
Narain, V., & Lally, C. (2025). Consumer wearable devices and disease prevention (POSTnote 741). UK Parliamentary Office of Science and Technology. https://doi.org/10.58248/PN741

Narain, V., & Lally, C. (2025). Consumer wearable devices and disease prevention (POSTnote 741). UK Parliamentary Office of Science and Technology. https://doi.org/10.58248/PN741

Privacy International. (2020). No body's business but mine: How menstruation apps are sharing your data. https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data

Radanliev, P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. Frontiers in Digital Health, 7, Article 1431246. https://doi.org/10.3389/fdgth.2025.1431246

Redhead, C. A. B., Bowden, C., Ainsworth, J., Burns, N., Cunningham, J., Holm, S., & Devaney, S. (2025). Unlocking the promise of UK health data: Considering the case for a charitable GP data trust. Medical Law Review, 33(1), Article fwae043. https://doi.org/10.1093/medlaw/fwae043

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2025/327 of the European Parliament and of the Council of 22 January 2025 on the European Health Data Space. Official Journal of the European Union, L 2025/327. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0327

Smith, C., Boyd, A., Pagel, C., & Morris, A. (2026). Trust, not technology: Governing access to health data as the decisive challenge for the UK. The Lancet Digital Health, 7, e145–e147. https://doi.org/10.1016/S2589-7500(26)000178

Sterckx, S., Rakic, V., Cockbain, J., & Borry, P. (2016). "You hoped we would sleep walk into accepting the collection of our data": Controversies surrounding the UK care.data scheme and their wider relevance for biomedical research.

Medicine, Health Care and Philosophy, 19(2), 177–190. https://doi.org/10.1007/s11019-015-9661-6
Takka, A.-M. (2023). A deep dive into dynamic data flows, wearable devices, and the concept of health data.

International Data Privacy Law, 13(2), 124–140. https://doi.org/10.1093/idpl/ipad007

Thorogood, A., & Tovino, S. (2024). Interplay of EU regulatory frameworks: GDPR, Data Governance Act and European Health Data Space. Technology and Regulation, 2024, 143–158. https://doi.org/10.26116/techreg.2024.017

van Drumpt, S. (2025). Secondary use under the European Health Data Space: Setting the scene and towards a research agenda on privacy-enhancing technologies. Frontiers in Digital Health, 7, Article 1602101. https://doi.org/10.3389/fdgth.2025.1602101

Wiertz, S., & Boldt, J. (2024). Ethical, legal and practical concerns of implementing new forms of consent for health data research: A qualitative interview study. Journal of Medical Internet Research, 26, Article e52180. https://doi.org/10.2196/52180

Zhang, J., Morley, J., Gallifant, J., Oddy, C., Teo, J. T., Ashrafian, H., Delaney, B., & Darzi, A. (2023). Mapping and evaluating national data flows: Transparency, privacy, and guiding infrastructural transformation. The Lancet Digital Health, 5(10), e737–e748. https://doi.org/10.1016/S2589-7500(23)00157-7

Zulueta, P. (2021). Confidentiality, privacy, and general practice: GPDPR and the brave new world of 'big data'. British Journal of General Practice, 71(710), 420–421. https://doi.org/10.3399/bjgp21X717017