informatics

MDPI

Article

Perceptions of Wearable Health Data Governance Among Wearable Users and Health Professionals in South Africa

Lydia Osarugue Izu *, Brenda Scholtz and Ifeoluwapo Fashoro

Department of Computing Sciences, Nelson Mandela University, Gqeberha 6001, South Africa; brenda.scholtz@mandela.ac.za (B.S.); ife.fashoro@mandela.ac.za (I.F.)
* Correspondence: lydiabenizu@gmail.com

Abstract

Personal health management and clinical health systems are increasingly being transformed by data-driven smart technologies that enable remote monitoring, predictive analytics, and digitally mediated care. Wearable technologies contribute to this transformation by continuously generating wearable health data (WHD), but integrating such data into routine and clinical health management raises governance requirements beyond those for traditional health data. This study examines perceptions of WHD governance among wearable users and health professionals in South Africa. A mixed-methods approach was adopted, with quantitative and qualitative data collected through questionnaires and interviews. The findings show that wearable users are generally confident in WHD governance regarding access, reliability, trust, accuracy, and sharing. Privacy and third-party data practices raised comparatively less concern, though with less certainty, while perceptions of security and the adequacy of current South African laws were less definite and marked more by uncertainty. Health professionals viewed WHD governance more cautiously, emphasising regulatory adequacy, data quality, security, accountability, and the conditions required for meaningful use of WHD in health management. The study concludes that effective WHD governance requires more than formal regulation and must also support intelligibility, credibility, quality assurance, and practical oversight to support the responsible integration of WHD into health management.

Keywords: wearable health data; data governance; governance perceptions; data privacy; data quality; data security; accountability; health management

Check for updates

Academic Editor: Antony Bryant

Received: 29 May 2026
Revised: 30 August 2026
Accepted: 2 September 2026
Published: 4 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

As wearable technologies, or wearables, are increasingly valued for their role in supporting health management through the generation of wearable health data (WHD), the governance of such data, and how that governance is perceived, become equally important [1–5]. Wearables refer to electronic devices worn on the body that collect, transmit, and display data in real time, including fitness trackers, smartwatches, smart glasses, and wearable electroencephalography devices [6]. Advancements in technology have led to a progressive increase in the number of wearables available and in the complexity of their functions and roles [7]. This has, consequently, contributed to the expansion of digital health technologies that enable the continuous, real-time collection of health-related data outside traditional clinical settings, thereby creating new opportunities for preventive care, patient monitoring, personalised health management, and clinical decision-making [8–12]. Within this broader digital health innovation, wearables also contribute to smart health

monitoring and healthcare, as they enable more continuous and connected forms of health observation and management [9,13]. In contexts characterised by strained healthcare systems and rising burdens of chronic conditions, such as in South Africa and other low-income countries [14–16], these developments present meaningful opportunities to extend care beyond institutional clinical settings [17,18]. Even more so, some studies have reported the potential of wearables through WHD to support chronic disease management [19,20] and a broader global health goal [21].

On the other hand, integrating WHD into health management introduces unique data management (DM) concerns that fuel complex governance requirements and shape perceptions of governance among key stakeholders [5]. WHD management refers to the processes involved in acquiring, transferring, storing, processing, analysing, and disseminating wearable health data across its lifecycle [22–24]. DM concerns related to data quality, security, and privacy challenges are reported as major concerns regarding the use of wearables for collecting and analysing unique and sensitive data such as WHD [25–29]. Particularly for healthcare professionals and users, privacy and security concerns are at the forefront of their considerations when integrating WHD into clinical and self-health management, and these concerns are further compounded by governance mechanisms and policies lagging behind rapidly emerging technological innovations [5,30]. Unlike conventional clinical data, WHD is continuously generated, often processed across multiple platforms, and may be shared with a range of actors, including technology providers, third-party applications, and healthcare professionals [31]. This raises concerns about data access, ownership, consent, transparency, and accountability, all of which are key governance aspects [1,32–34]. Thus, although wearables are useful because they can collect routine health-related data over extended periods and in largely unobtrusive ways, the same characteristics also increase the governance requirements and complexity of WHD [2,35,36].

According to [31], WHD governance primarily aims to ensure effective data access, promote data-driven engagement, and foster trust in data stewardship in line with established privacy policies. More broadly, data governance (DG), as a subset of data management, concerns the exercise of authority, control, decision rights, and accountability over data-related matters [37,38]. Existing legal and regulatory instruments, such as the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and the Protection of Personal Information (POPI) Act, provide important governance foundations [35,36,39–42]. However, the novel, dynamic, and distributed nature of WHD raises questions about whether such instruments adequately address the practical realities associated with it. Winter and Davidson [42] further show that patient-generated health data operate across overlapping regulatory regimes, creating uncertainty about what rules apply and where governance gaps may remain. Relatedly, Ref. [43] argue that, as the evidence base for the use of wearables in chronic disease management is strengthened, several challenges still need to be overcome before widespread adoption can occur in healthcare settings, including stringent regulatory approval, data privacy and confidentiality, and software accuracy. To this end, there are calls for the development of context-relevant, stakeholder-aligned and collaboratively informed new guidelines and rules to support effective governance of WHD [35].

Building on [30], understanding perceptions of WHD governance is therefore considered important not only for identifying gaps or concerns with such governance but also for informing the development and implementation of appropriate governance mechanisms and requirements. Perceptions of WHD governance reflect how governance arrangements surrounding WHD are interpreted, evaluated, and judged. They reveal concerns about the management of WHD while also helping to establish what is considered appropriate governance for such data. Drawing on [44], such perceptions are shaped not only by

observed practices but also by context, personal experience, and expectations. Particularly, privacy perceptions around WHD are highly context-dependent, influenced by personal and technological factors such as trust, attitudes towards innovations, users' health status, familiarity with the device, device type, the nature of the data collected, and the parties with whom the data may be shared, and therefore often differ across users [45]. Governance arrangements that are misaligned with these perceptions may undermine trust, constrain adoption, and limit the meaningful integration of WHD into health management, since, according to [34,46,47], DG is central to defining access rights, ownership, sharing modalities, transparency, and the effectiveness of WHD use in clinical and non-clinical contexts. Deliberate and appropriate governance measures can enhance confidence in WHD, support its legitimacy, and enable its benefits to be more fully harnessed, whereas inadequate governance may leave WHD underused, siloed, or regarded as illegitimate, particularly in clinical contexts [23,34,48–50].

Previous studies on wearables have examined issues such as wearable adoption in healthcare [51–53], attitudes and perceptions towards the use of wearables in health management, as it relates to the potential benefits and associated concerns of the health data they generate, including calls for effective WHD management and governance [1,5,8,35,36,54–56]. Less attention has, however, been paid to how key WHD stakeholders, such as wearable users and health professionals, perceive WHD governance. WHD governance involves multiple WHD stakeholders, broadly understood as persons or groups with a stake in the potential value of WHD and who are affected by the practices and policies relating to its access and use [31]. Among these, wearable users and health professionals are closely implicated in the generation, use, and health-related application of WHD [31,57], and are thus particularly important to this study.

With the limited attention given to how wearable users and health professionals perceive the governance of WHD itself, there is therefore an important empirical gap in achieving the much-needed effective WHD governance, particularly in settings such as South Africa, where digital health opportunities coexist with a regulatory gap in WHD governance and healthcare system constraints. This study, therefore, examines perceptions of WHD governance among wearable users and health professionals, with a limited geographical scope in South Africa. The study considered wearable use broadly in relation to health-related data collection and management and was not restricted to particular diseases, wearable types, or contexts of use. In the bigger picture, it seeks to contribute to the development of governance approaches that are contextually relevant and responsive to the realities of data-driven health environments and key stakeholders. Insights into perceptions of governance are therefore relevant not only to wearable users and health professionals but also to broader actors involved in WHD governance. This is especially so for data governance authorities, wearable manufacturers, and technology policymakers, whose decisions determine how WHD is accessed, shared, protected, and used in practice [31,34,58–60]. Accordingly, the study addresses the following main research question: What are the perceptions of WHD governance among wearable users and health professionals in South Africa?

The remainder of this paper is structured as follows. Section 2 discusses related literature. Section 3 explains the research methodology. The results and findings are presented and discussed in Sections 4 and 5, respectively, while Section 6 presents the study limitations, and Section 7 concludes the paper.

2. Literature Review

2.1. WHD in Health Management and WHD Management Concerns

Wearables' usefulness in health management is realised through the data they collect; therefore, WHD constitute a central data asset and informational resource through which much of the value of wearables is realised in health management [31,40,61,62]. Wearables are products of technological advancements in sensors, artificial intelligence (AI), and the Internet of Things (IoT), which collect and analyse vast amounts of essential data [48,63–66]. The ability to continuously collect physiological, behavioural, and activity-related data outside traditional clinical environments has made wearables increasingly important in health management [40]. Literature shows that wearables through WHD are relevant across a wide range of health-related contexts, including monitoring, prevention, diagnosis support, treatment support, and broader health research [61,62]. Their value in health management is closely linked to their ability to support more continuous and contextually rich understandings of health. Unlike episodic data gathered during consultations, WHD can extend health observation into everyday life and provide ongoing insight that may support preventive care, self-monitoring, patient engagement, and chronic disease management [5,7,61]. In this way, WHD contributes to a more continuous model of health management in which health data can be generated, accessed and used beyond the boundaries of traditional clinical encounters.

The potential of wearables and WHD in chronic disease management has been emphasised and reported in several studies. Asif and Gaur [54], for example, posit that advances in digital health technologies such as wearables may reform the management of chronic diseases, especially diabetes and cardiovascular diseases, in ways that support more personalised and equitable healthcare. In the South African context, where chronic diseases form part of the broader burden weighing on the healthcare system, wearables through WHD may also support preventive health management by encouraging healthier lifestyles, improving physical activity, and enabling users to monitor indicators such as steps taken, calories burnt, heart rate, blood pressure, food intake, and water intake [67]. These possibilities suggest that wearables and WHD can support health management through both direct health monitoring and the promotion of healthier behaviours.

According to Alaboud et al. [8], clinicians viewed patient-generated health data such as WHD as potentially valuable for improving ischaemic heart disease management. Their study showed that home-based tracking of blood pressure, weight, physical activity, and blood glucose was regarded as especially useful, particularly because such data could extend clinicians' visibility into patients' health status between visits, support earlier intervention and out-of-hospital care. Importantly, the study also showed that the value of these data did not lie in raw data capture alone, but in their accessibility, integration into electronic health records, meaningful visualisation, and clinical actionability. Clinicians prefer the standardised collection of WHD, which can be easily and ethically integrated into existing health care systems, together with visualisations such as dashboards, trend graphs, and automated alerts that could help identify health deterioration quickly, while avoiding burdensome raw data streams that increase workload [8]. These perspectives from [8] reinforce the point that WHD is most useful in health management when it is accessible, interpretable, and supports decision-making in practice.

As wearable use expands, so too does the importance of understanding how WHD is collected, handled, interpreted, and used, which creates a necessary transition from the value of wearables and WHD in health management to the management of WHD itself. WHD management encompasses the handling of WHD from acquisition to dissemination, with its lifecycle typically beginning at sensor-based data collection and extending through pre-processing, transfer, storage, and analysis [22,23]. After collection, WHD is commonly

transmitted, either directly or through installed applications, to designated servers or cloud-based platforms for storage and analysis, with computers and smartphones often serving as middleware that support intermediate storage, feedback, and onward transfer within the wearable data ecosystem [23,24,47]. As a result, WHD typically moves through a broader data ecosystem rather than remaining confined to a device, which means that its management is not simply a technical matter, but part of a wider environment in which questions of control, responsibility, and appropriate use arise [1,42,68].

Concerns surrounding the use of wearables for WHD arise largely from the data-related risks associated with how these data are managed rather than from the devices alone. These concerns, which are interconnected and often overlap, relate to data storage, privacy, ownership, use, sharing, security, access, quality, and governance [32,64]. The overlapping nature of WHD management concerns and their driving factors, such as the data sensitivity and complex management ecosystem, indicate that managing WHD is not merely about moving data through a technical lifecycle, but also about managing sensitive data in ways that preserve control, protection, and acceptable use across a broader digital ecosystem and among stakeholders. Furthermore, the literature demonstrates that the interrelated concerns of WHD management return attention to WHD governance, which is regarded not only as a concern in itself but also as a necessary means of addressing other WHD management concerns by defining standards, responsibilities, access conditions, and broader rules for the appropriate handling of WHD [32,46,58,64,65,69–72].

2.2. WHD Governance

DG, as a subset of data management, concerns the exercise of authority, control, decision rights, and accountability over data-related matters [37,38]. By contrast, DM refers to the broader processes involved in handling data across its lifecycle, including its planning, creation, storage, use, maintenance, and disposal [37]. In this sense, DG provides the rules, responsibilities, and oversight through which DM is directed and controlled. WHD governance emerges within the broader governance of health data, but it must also respond to WHD's distinctive characteristics as well as management mechanisms and expectations. Although the governance of traditional and other electronic health data has long focused on issues such as privacy, confidentiality, access, stewardship, accountability, and compliance, WHD introduces additional complexity to its governance requirements [31,34]. Due to its unique and multi-stakeholder management mechanisms, WHD presents a new and complex DG paradigm that draws together the health, technology, public, and commercial sectors, while also requiring governance arrangements capable of evolving alongside emerging opportunities associated with the data and management requirements [31,73,74]. Drawing on DG definitions from [37,72,75], WHD governance may be understood as the exercise of authority, control, decision rights, and accountability over WHD and its management, through the policies, roles, responsibilities, and oversight mechanisms that determine how WHD is accessed, used, shared, protected, and otherwise handled across its lifecycle.

The complexity of WHD governance is compounded by the fact that current regulatory and governance arrangements do not always align with the realities of WHD. WHD is not automatically governed in the same way as traditional personal health data, but is instead often mediated by the private policies and technical architectures of wearable manufacturers and their partners [73,74]. To this end, Refs. [36,41] note that WHD remains largely unregulated. The literature suggests that existing personal and health data regulations remain limited in adequately governing WHD, even in jurisdictions with relatively advanced data protection regimes [2,36,41,73,74]. In particular, DG measures such as the POPI Act in South Africa and the GDPR in the European Union are intended to govern personal

data, including health data, yet their application and adequacy in the context of WHD remain constrained [2,41,73,74]. This constraint stems in part from the emergent nature of the WHD management model and the continually changing capabilities of wearables in collecting and analysing health data [2].

The governance of WHD is unavoidably multi-stakeholder in nature. These stakeholders include wearable users, health professionals, manufacturers and their partners, information technology vendors, and technology and data regulators, with uneven and often undefined authorities, roles, and responsibilities [31,73,74]. There is, therefore, a governance challenge that is not merely technical or regulatory, but also relational, since these stakeholders do not occupy equal positions of power, control, or benefit within the WHD management and governance ecosystems [42,73]. For instance, although wearable users generate the health data, the data themselves often reside within manufacturer-controlled or partner-controlled cloud infrastructures, with these users ceding, willingly or otherwise, significant governance rights and responsibilities in the course of using their devices and the associated services [24,73]. The governance imbalance among stakeholders, drawing on [76], extends beyond concerns about safeguarding WHD privacy and governance rights to include the exclusive proprietary rights that manufacturers and their partners exert over the WHD generated and managed through their wearable products. Such exclusivity can hinder purpose-driven WHD sharing for broader societal benefits, including research and improvements to inter-organisational systems [76]. As a result, the opportunities offered by wearables through WHD in health management remain closely tied to how effectively concerns surrounding WHD management are addressed. To this end, effective management of WHD is closely linked to the extent to which users feel empowered to manage privacy, trust, and acceptable risk [68]. According to the literature, this is where WHD governance becomes important in driving and directing the course of effective WHD management, in ways that help allay concerns, build confidence and sustain meaningful use [31,32,34,77,78].

The unevenness in stakeholders' positions within the WHD use and management ecosystem, and the broader governance imbalance in the distribution of authority, responsibility, power, control, and benefit, also means that stakeholders approach WHD governance with conflicting interests and values for the data. Manufacturers of wearables and their partners are often positioned as more powerful stakeholders within WHD governance, with stronger stakes in the data and with norms, values, and interests that can differ significantly from those of other actors [73] (47–48). For wearable users, WHD represents a source of health monitoring and management, whereas for wearable manufacturers and their partners, the same data may also signify commercial value through data analytics, advertising access, or other forms of monetisation [73,79]. The conflicting interests and values complicate achieving governance goals as well as intensify concerns about privacy, security, ownership, and the fair distribution of benefits from WHD, especially in the absence of harmonised regulatory requirements and clear governance expectations [31,42,73,80].

The goals of WHD governance remain broadly aligned with those of traditional and electronic health data governance, but with more dynamic and complex implications. Winter and Davidson [31] posit that the governance of health data generally aims to support compliance, efficiency, innovation, data-driven engagement, quality care, and trust. The authors similarly explain that in the specific context of WHD, the more immediate governance goals centre on enabling effective data access, fostering data-driven engagement, and building trust in the stewardship of WHD under appropriate privacy and access conditions. Protecting WHD remains a primary objective, and this is closely tied to access control, which is critical for safeguarding the data from unauthorised access while enabling appropriate use by authorised stakeholders [31,73]. Beyond protection, WHD governance

also seeks to maximise the value WHD provides to relevant stakeholders through effective, responsible, and trustworthy use [31,73].

On the technological front, WHD governance can advance the implementation of more interoperable and standardised tools that are easier to integrate into healthcare systems [78], while on the non-technological front, it can also drive the regulatory and governance changes needed to address existing concerns surrounding WHD [32,47,64,78]. Deliberate governance measures can therefore help define ownership and access conditions, reduce siloed use of WHD, improve transparency, and support the confidence necessary for the benefits of wearables to be more fully realised [23,34,49,58,60]. For this reason, several studies have called for more explicit governance responses to WHD. Existing work has recommended the formulation and implementation of regulations and governance measures as part of WHD governance strategies that clarify privacy, quality, ownership, use, and sharing, while also addressing the lack of harmonised and widely accepted governance approaches for WHD [31,32,34,42,45,47,58,64,73,74,77,78]. The suggestion is that WHD governance strategies should promote standardisation, quality, privacy, security, interoperability, and stakeholder-centred governance, while balancing innovation with the protection of data subjects and broader social value [31,34,42,80].

A conclusion that can be drawn from the literature is that DG plays a central role in defining data access, ownership, sharing modalities, transparency, and the effective use of WHD [34,46,47]. Furthermore, the literature indicates that WHD governance is both distinct and evolving, influenced by the characteristics of WHD itself, the multiplicity of stakeholders involved, and the uneven fit of existing governance arrangements. In this regard, the literature suggests that understanding perceptions of WHD governance among key stakeholders, such as wearable users and health professionals, may serve as an important starting point for advancing more effective and contextually appropriate governance, especially since such perceptions can illuminate how current arrangements are interpreted, where concerns remain unresolved, and what may be regarded as appropriate governance in practice [5,30,31,57]. Moreover, governance arrangements that are misaligned with stakeholders' perceptions may undermine trust, constrain adoption, and limit the meaningful integration of WHD into health management, especially in contexts where users may not have sufficient information to make privacy-sensitive decisions and where concerns about wearable use and integration remain visible in practice [5,30,57].

3. Research Methodology

3.1. Research Approach and Design

This study adopted a mixed methods research approach to examine perceptions of WHD governance in South Africa from the perspectives of wearable users and health professionals. A mixed methods approach was appropriate because the study sought both breadth and depth in understanding the phenomenon being studied, enabling the identification of broad patterns in governance perceptions among wearable users as well as contextual and practice-based insights from health professionals. In this regard, the study followed a convergent research design, in which quantitative and qualitative data were collected and analysed separately and then brought together in the interpretation to draw an evidential conclusion. The convergent design was suitable because, as posited by Creswell and Creswell [81], it supports a more comprehensive understanding of a research problem and enables the corroboration of views derived from different data sources.

3.2. Target Population and Sample

The target population for this study is aligned with the two components of the mixed methods approach and design adopted. For the quantitative component, the target pop-

ulation comprised wearable users in South Africa. For the qualitative component, the target population comprised health professionals in South Africa. Voluntary sampling was used to select the sample for the quantitative component. Voluntary sampling, also referred to as volunteer sampling, is a non-probability sampling technique in which individuals self-select to participate in a study by responding to a call for participation or advertisement [82,83]. The literature recognises voluntary sampling as a feasible and practical approach for identifying and accessing participants who may be difficult to locate through an available sampling frame [82,83]. The technique may, however, be susceptible to self-selection bias and may limit the statistical representativeness of the resulting sample. These limitations, according to [83,84], can be mitigated through measures such as predefined sampling criteria aligned with the research aim, broad and sustained recruitment, and attainment of an adequate sample size. Voluntary sampling was considered appropriate for this study because wearable users in South Africa were not easily identifiable, and no accessible sampling frame was available for probability sampling. To strengthen the relevance and reach of the sample, predefined inclusion criteria were applied, and recruitment was conducted both online and in person over approximately five months, from January to May 2024. For online recruitment, participation was advertised via social media and social network platforms such as LinkedIn, Facebook, X (formerly Twitter), WhatsApp, and Telegram, as well as online wearable technology forums. Respondents who met the study criteria and volunteered completed the online questionnaires. The inclusion criteria required respondents to reside in South Africa, be at least 18 years old, and have used or currently be using wearables for health-related data collection.

Purposive sampling was adopted for the qualitative component of the study because it enabled the deliberate selection of health professionals knowledgeable about WHD applications in health settings and able to provide relevant perspectives on its governance within such settings. According to [83,84], purposive sampling is a non-probability sampling technique in which participants are selected using the researcher's judgement to identify those considered most informative and best able to contribute to answering the research question(s) and meeting the research objectives. Apart from their inherent professional experience and knowledge of health data and health management, participants in the study were selected based on criteria related to their engagement with WHD in practice in South Africa. Thus, the criteria required them to be practising medical doctors in South Africa working with patients or individuals who use wearables to collect health data, seeing patients or individuals who have used WHD to manage their health, and having experience with the integration or use of WHD in health management. The resulting sample comprised six practising medical doctors, including three general practitioners, two cardiologists, and one general surgeon, all with more than 10 years of professional experience.

The qualitative component of the study was intended to provide in-depth professional perspectives, not to achieve statistical representation or numerical equivalence with the quantitative component. Accordingly, a sample size of six was considered appropriate and sufficient for the qualitative component, as Saunders et al. [83] indicate that qualitative studies involving in-depth interviews may comprise between five and 25 participants. The determination of the sample size also considered the feasibility of conducting in-depth interviews, since, as explained by Walliman [85], an appropriate qualitative sample size should be balanced against available research resources, including time, cost, and effort. The six purposively selected health professionals, therefore, constituted a manageable sample from which the in-depth professional perspectives required for this component could be obtained.

3.3. Data Collection and Analysis

Quantitative data were collected from a sample of wearable users in South Africa through an online questionnaire. The questionnaire included items on respondents' demographic and user profiles; general perceptions of WHD governance; reasons for trusting WHD; familiarity with South African laws/Acts and their goals; perceptions of the South African laws/Acts applicable to WHD regulation; and engagements with wearable privacy and data sharing policy statements. It also contained specific WHD governance-related items, including access, sharing, trust, reliability, accuracy, privacy, security, and the perceived adequacy of relevant laws and regulations. Five-point and three-point Likert scales were used for WHD governance-related items that required respondents to indicate the extent of their perceptions or agreement, while binary categorical measures were used for items that did not require rating. A total of 204 questionnaires were completed and included in the analysis. Responses to individual questionnaire items were not mandatory, and respondents could skip items where necessary; consequently, the number of valid responses varied across some items and analyses.

The quantitative data were analysed using descriptive and inferential statistics. Descriptive statistics were used to summarise data on respondents' profiles and governance-related perceptions in frequencies and percentages. The inferential analysis focused on the combined items within four of the aspects or factors relating to WHD governance, namely general perceptions regarding WHD governance, trust regarding WHD, familiarity regarding WHD-related laws/acts, and perceptions of laws/acts regulating WHD. The internal consistency of these factors was assessed using Cronbach's alpha, yielding coefficients of 0.72, 0.71, 0.75, and 0.71, respectively. Where applicable, items originally measured on a three-point Likert scale were transformed to a five-point scale using the transformation formula $(2x - 1)$ to enable meaningful comparability and interpretation across the measured factors. Additionally, negatively worded items within the "general perceptions on WHD governance" factor were reverse-coded to maintain a consistent scoring direction. To determine the mean score, composite mean scores were calculated for each respondent by averaging their scores on the questionnaire items within each factor. These scores were then used to calculate the mean and standard deviation for the overall sample and for the demographic and user profile groups. Given the sample sizes applicable to the quantitative analysis of the study and specifically the parametric tests, formal normality testing was not considered necessary, as the *t*-test and *F*-test are robust to departures from normality with sufficiently large samples. According to Cohen et al. and Gravetter and Wallnau [86,87], normality is generally not a concern for parametric tests such as *t*-tests and ANOVA with large samples, as large samples tend to produce approximately normal sampling distributions of means, while these tests are robust to departures from normality under such conditions.

Univariate Analysis of Variance (ANOVA) was used to determine whether the mean scores of the four governance-related factors differed significantly across gender, age, technological capability, and wearable use experience. The ANOVA included only cases with complete data for the demographic variables and governance-related factors, resulting in an analysis sample of 198 respondents. All inferential analyses were conducted at a 95% confidence level, with statistical significance determined at $p < 0.05$. The *F*-value was used to assess the ratio of between-group to within-group variance, drawing on Cohen et al. and Gravetter and Wallnau [86,87]. Where statistically significant differences involved variables with three or more group levels, Scheffé post hoc tests were conducted to identify the specific groups between which differences occurred. For comparisons involving two groups, a *t*-test was used. Cohen's d was calculated for pairwise comparisons to assess the practical magnitude of statistically significant differences. Values from 0.20 to 0.49 were interpreted

as small effects, values from 0.50 to 0.79 as medium effects, and values of 0.80 and above as large effects, following recommendations in [86,87]. The chi-square test was applied to examine the associations between wearable use experience and familiarity with WHD-related laws/acts, as well as perceptions of laws/acts regulating WHD. Cramér's V was used to assess the strength of statistically significant chi-square associations. Pearson correlation analysis was used to examine the direction and strength of relationships among the governance-related factors. Microsoft Excel 365 and Statistica Version 14.0.0.15 were used for the quantitative data analyses.

The qualitative component of the study employed semi-structured interviews with the six purposively sampled health professionals identified in the qualitative findings section of the paper (Section 4.2), using the unique codes HP1-HP6. The interviews explored perceptions of existing WHD governance, governance concerns in the management and use of WHD, and possible governance responses. To analyse the qualitative data, thematic analysis was adopted, drawing on the processes outlined by [88–90]. The data were coded and organised into thematic categories relevant to the paper's focus, supported by the Atlas.ti software version 24.1.1.

Results and findings from the quantitative and qualitative data were integrated in the discussion to provide a fuller understanding of how WHD governance is perceived and what those perceptions imply for strengthening governance in South Africa.

3.4. Ethical Considerations

Ethical principles relating to informed consent, confidentiality, and anonymity were observed throughout the study. Before the study's commencement, applicable institutional ethics approval was sought and obtained with ethics Approval number 2023-SCI-0233. Participation in both components of the study was voluntary. For the quantitative component, a recruitment information sheet and an electronic informed consent form were included with the online questionnaire, and participants could not proceed to complete the questionnaire without providing consent. These informed respondents about the nature and purpose of the study, voluntary participation, and their right to discontinue participation before submitting their responses. For the qualitative component, participants received an information sheet explaining the study aim, their role in the research, and the potential benefits and risks of participation. Participants who agreed to participate completed and returned a consent form before being interviewed. The consent form also explained their right to withdraw without any implications and the researcher's commitment to confidentiality. Questionnaire responses were collected anonymously. No identifiable information that could be used to trace responses to individual respondents was requested through the questionnaire or its online properties. The identities of the interview participants were known to the researcher and therefore could not be anonymous; however, these were kept confidential and were not disclosed in the analysis or reporting. Pseudonymous participant codes (HP1–HP6) were used to anonymise the interview data, and no identifiable information was included in the reported findings.

4. Results

This section presents the quantitative results and qualitative findings of the study on perceptions of WHD governance among wearable users and health professionals in South Africa. It is organised into two subsections. The first presents the quantitative results on wearable users' perceptions of WHD governance, while the second presents the qualitative findings on health professionals' perceptions of WHD governance.

4.1. Quantitative Results on Wearable Users' Perceptions of WHD Governance in South Africa

This subsection presents the quantitative results on wearable users' perceptions of WHD governance in South Africa. It begins with respondents' demographics and user profiles, followed by the main results on governance-related perceptions and familiarity with relevant laws, and an inferential analysis of governance-related factors.

4.1.1. Respondents' Demographic and User Profile

A total of 204 responses were received. Data on gender were provided by 203 respondents, of whom 131 (64.5%) were female, and 71 (35.0%) were male, while one respondent preferred not to disclose gender. Data on age were provided by 202 respondents. The largest age group was 18–29 years (n = 71, 35.0%), followed by 30–39 years (n = 46, 23.0%), while respondents aged 40–49 and 50–59 each accounted for 34 (16.8%). Smaller proportions were aged 60–69 (n = 14, 6.9%) and above 70 (n = 3, 1.5%). In terms of technological capability, 115 respondents (56.4%) rated themselves at a high level and 71 (34.8%) at a satisfactory level. Wearable use experience showed a similar pattern, with 89 respondents (43.6%) rating their experience as satisfactory and 79 (38.7%) as high. Overall, the sample was largely female, relatively young, and generally confident in both digital technology use and the experience of using wearables.

4.1.2. General Perceptions of WHD Governance

The general perception results shown in Table 1 are based on respondents' ratings of the governance-related items on a five-point Likert scale, ranging from strongly disagree to strongly agree. The results indicate that respondents viewed several aspects of WHD governance favourably, especially access, reliability, trust, accuracy, and sharing. Relevant keywords are bolded to highlight items related to each of these aspects. Access received the strongest positive rating, with 119 respondents (58.3%) agreeing and 46 (22.5%) strongly agreeing that they had access to the health data collected by their wearable, yielding a combined positive rating of 80.8%.

A related pattern emerged regarding users' perceived ability to grant access to their WHD, where 76 respondents (37.3%) agreed and 29 (14.2%) strongly agreed that they could grant access to the health data collected by their wearable to anyone as they deemed fit, yielding a combined positive rating of 51.5%, although 43 respondents (21.1%) remained neutral. Reliability was also rated highly, with 130 respondents (63.7%) agreeing and 28 (13.7%) strongly agreeing that their WHD was reliable, yielding a combined positive rating of 77.4%. Trust in WHD was similarly positive, with 116 respondents (56.9%) agreeing and 24 (11.8%) strongly agreeing to trusting the health data collected by their wearables. Data accuracy also received a high positive rating, with 113 respondents (55.4%) agreeing and 23 (11.3%) strongly agreeing. Sharing also received a high positive rating, where the majority of the respondents provided a combined positive rating of 125 (61.3%), with 92 respondents (45.1%) agreeing and 33 (16.2%) strongly agreeing that they could share the health data collected by their wearable, while 44 respondents (21.6%) remained neutral. These findings suggest that respondents generally perceived their WHD as accessible, usable, and reasonably dependable.

The results of the follow-up item on why respondents trust their WHD in Table 2 help shed more light on what underpins some of the positive patterns reported in Table 1. The strongest reason for trusting WHD was their perceived reliability, with 114 respondents (56%) agreeing and 30 (15%) strongly agreeing, yielding a combined positive rating of 71%. Accuracy and accessibility followed with equal combined positive ratings of 63%, while validity was positively rated by 61% of respondents. By contrast, shareability elicited a much weaker positive response, where only 28% agreed that they trusted WHD because it

was easily shareable, while 46% remained neutral. These results suggest that trust in WHD was grounded primarily in respondents' views of the data as reliable, accurate, accessible, and valid, rather than in its portability or exchangeability.

Table 1. General Perceptions of WHD Governance (n = 204).

Statements on WHD Governance	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
I have **access** to the health data collected by my wearable	4 (2.0%)	9 (4.4%)	26 (12.7%)	**119 (58.3%)**	46 (22.5%)	204 (100.0%)
I can **share** the health data collected by my wearable	8 (3.9%)	27 (13.2%)	44 (21.6%)	**92 (45.1%)**	33 (16.2%)	204 (100.0%)
South Africa **requires increased regulations** to protect data collected by wearables	6 (2.9%)	11 (5.4%)	**89 (43.6%)**	65 (31.9%)	33 (16.2%)	204 (100.0%)
I am concerned about the **privacy** of the data collected by my wearable	22 (10.8%)	**60 (29.6%)**	44 (21.7%)	47 (23.2%)	30 (14.8%)	203 (100.0%)
I can **grant access** to the health data collected by my wearable to anyone as I deem fit	11 (5.4%)	45 (22.1%)	43 (21.1%)	**76 (37.3%)**	29 (14.2%)	204 (100.0%)
I consider the health data generated by my wearable **reliable**	1 (0.5%)	9 (4.4%)	36 (17.6%)	**130 (63.7%)**	28 (13.7%)	204 (100.0%)
I **trust** the health data collected by my wearable	1 (0.5%)	8 (3.9%)	55 (27.0%)	**116 (56.9%)**	24 (11.8%)	204 (100.0%)
I am concerned that a **wearable device manufacturer, company or one of their partners** may analyse or track my health data analytics	21 (10.3%)	**65 (31.9%)**	54 (26.5%)	40 (19.6%)	24 (11.8%)	204 (100.0%)
I consider the health data collected by my wearable to be **accurate**	1 (0.5%)	11 (5.4%)	56 (27.5%)	**113 (55.4%)**	23 (11.3%)	204 (100.0%)
My wearable health data is adequately secured by the manufacturers of my wearable	5 (2.5%)	12 (5.9%)	**96 (47.1%)**	76 (37.3%)	15 (7.4%)	204 (100.0%)
In South Africa, there are adequate laws protecting the privacy of health data gathered through wearables	10 (4.9%)	31 (15.2%)	**111 (54.4%)**	43 (21.1%)	9 (4.4%)	204 (100.0%)

Note: The calculated percentages in Table 1 are based on the valid row total and rounded to one decimal place; therefore, some rows may not total 100.0% due to rounding. Bold values indicate the highest response category for each item on this table and other tables where such formatting is used.

Table 2. Reasons for Trusting WHD (n = 204).

Statements on Trust Reasons	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Because they are reliable, i.e., data is consistent over time and across other device measurements	2 (1%)	13 (6%)	45 (22%)	**114 (56%)**	30 (15%)	204 (100%)
Because they are accurate, i.e., they correspond with actual reality	3 (1%)	14 (7%)	59 (29%)	**102 (50%)**	26 (13%)	204 (100%)
Because they are readily accessible	9 (4%)	24 (12%)	43 (21%)	**106 (52%)**	22 (11%)	204 (100%)
Because they are valid, i.e., they correspond with the measured attributes	2 (1%)	14 (7%)	64 (32%)	**105 (52%)**	18 (9%)	203 (100%)
Because they are easily shareable	19 (9%)	34 (17%)	**94 (46%)**	49 (24%)	8 (4%)	204 (100%)
Other reasons	85 (45%)	**50 (26%)**	43 (23%)	6 (3%)	6 (3%)	190 (100%)

Table 1 shows that perceptions regarding privacy, third-party analytics, security, and regulation exhibit more variations. In relation to WHD privacy, the concern is less but

reflects non-negligible uncertainty, with 82 respondents (40.4%) disagreeing, 77 (38.0%) agreeing, and 44 (21.7%) remaining neutral that they are concerned about the privacy of their WHD. The concern that wearable manufacturers, companies, or their partners may analyse or track WHD attracted the highest overall negative response, with 86 respondents (42.2%) disagreeing, 64 (31.4%) agreeing, and 54 (26.5%) remaining neutral, which likewise reflects a comparatively lower concern in this aspect, though again with non-negligible uncertainty. Security reflected a somewhat different pattern with greater uncertainty, as 96 respondents (47.1%) remained neutral on whether wearable manufacturers adequately secured their WHD. In contrast, 91 (44.7%) agreed that manufacturers adequately secured their WHD, and 17 (8.4%) disagreed, showing a pattern of lower concern for WHD security but greater uncertainty than present for access, trust, reliability, and accuracy.

Regulatory perceptions were similarly tentative, as shown also in Table 1. Nearly half of the respondents, 98 (48.1%), agreed that South Africa requires increased regulation to protect WHD, while 89 (43.6%) remained neutral and only 17 (8.3%) disagreed. Likewise, only 52 respondents (25.5%) agreed that there are adequate laws in South Africa protecting the privacy of WHD gathered through wearables, whereas 111 (54.4%) remained neutral and 41 (20.1%) disagreed.

4.1.3. Familiarity with Relevant South African Laws and Their Perceived Applicability to WHD

The purpose of this item was to assess respondents' familiarity with selected South African legal instruments that may be relevant to WHD governance through their protection of rights relating to privacy, access to information, consumer protection, and health information. At this stage, respondents were asked about their familiarity with the legal instruments and their goals, rather than to assess their applicability to WHD. The South African Constitution was included because its protections of the rights to privacy and access to information provide an overarching rights basis relevant to the collection, use, sharing, and protection of personal and health-related data, including WHD. Respondents showed uneven familiarity with South African laws and acts that could potentially influence WHD governance. As shown in Table 3, the POPI Act had the highest level of familiarity, with 115 respondents (56%) indicating partial familiarity and 74 (36%) indicating complete familiarity. The Consumer Protection Act (CPA) and the South African Constitution (SAC) showed similar patterns of stronger partial familiarity rather than complete familiarity. By contrast, the Promotion of Access to Information (PAI) Act and the National Health Act (NHA) were less familiar, with 45% and 41% of respondents, respectively, indicating no familiarity at all. These results suggest that respondents' awareness of legal frameworks potentially relevant to WHD governance was uneven and strongest around the more visible and widely discussed instruments, especially the POPI Act.

Table 3. Familiarity with South African Laws/Acts and their Goals (n = 204).

Familiarity with South African Laws/Acts	No	Yes, but Not Completely	Yes, Completely
Protection of Personal Information (POPI) Act	15 (7%)	115 **(56%)**	74 (36%)
Consumer Protection Act (CPA)	29 (14%)	140 **(69%)**	35 (17%)
The South African Constitution (SAC)	33 (16%)	131 **(64%)**	40 (20%)
Promotion of Access to Information (PAI) Act	91 **(45%)**	84 (41%)	29 (14%)
National Health Act (NHA)	84 (41%)	103 **(50%)**	17 (8%)

When asked whether these laws and acts regulate WHD, the POPI Act emerged as the framework most strongly considered as applicable to WHD regulation, with

148 respondents (73%) believing that it completely regulates WHD, as shown in Table 4. Views on the other laws and acts were more divided. PAI Act and the CPA were each seen by roughly two-fifths of respondents as completely regulating WHD, while the SAC and the NHA were more often regarded as only partially relevant. These results indicate that respondents most strongly associated WHD regulation with data protection law, while the role of broader legal instruments remained less settled.

Table 4. Applicable South African Laws or Acts for WHD Regulation (n = 204).

Potential South African Laws or Acts for WHD Regulation	No	Yes, but Not Completely	Yes, Completely
Protection of Personal Information (POPI) Act	19 (9%)	37 (18%)	**148 (73%)**
Promotion of Access to Information (PAI) Act	29 (14%)	**88 (43%)**	87 (42.6%)
Consumer Protection Act (CPA)	39 (19%)	79 (39%)	**86 (42%)**
The South African Constitution (SAC)	52 (25.5%)	**85 (41.7%)**	67 (32.8%)
National Health Act (NHA)	40 (20%)	**113 (55%)**	51 (25%)

The uneven regulatory awareness and applicability perceptions reflected in Tables 3 and 4 should also be read alongside the results on respondents' engagement with wearable privacy and policy statements displayed in Table 5. The item in the questionnaire for which the data are presented in Table 5 referred to privacy statements or policies linked to the wearable or its associated application. More than half of respondents (113, 55%) reported not reading the privacy statements or policies of their wearables or wearable apps, while 75 (37%) read them only sometimes, and only 16 (8%) always read them.

Table 5. Reading Wearable Privacy Statements (n = 204).

Response to Reading Privacy Statement or Policy	Frequency	Percentage
No.	113	55%
Yes, but not always.	75	37%
Yes, always.	16	8%
Total	204	100%

As shown in Table 6 among the 188 respondents who did not read privacy policies and statements consistently, 146 (78%) said the policies were too long, 96 (51%) believed there was no point in reading them because they could not change any privacy settings, 52 (28%) found the wording difficult to understand, and 29 (15%) did not care how the company uses their data. These results show that limited legal and policy engagement may not be driven solely by familiarity with formal laws, but also by low confidence in the usefulness and accessibility of the policy documents through which data practices are communicated.

Respondents' interpretations of sample data use and sharing policy statements further reveal uncertainty and ambivalence in policy engagement and understanding, as shown in Tables 7 and 8. Table 7 presents respondents' reactions to a sample data usage and privacy statement, while Table 8 presents their interpretations of a sample data-sharing statement. When presented with a data usage statement indicating that collected information may be used for service provision, user interaction analysis, trend tracking, customer support, data analysis, research, and the development of new features, respondents were asked to indicate how the statement made them feel. The largest group, 105 respondents (51%), reported indifference. In contrast, 39 (19%) felt happy, 36 (18%) felt concerned, 23 (11%) felt safe, and 12 (6%) felt confused.

Table 6. Reasons for not Reading Privacy Statements or Policies (n = 188).

Reasons for Not Reading Privacy Statements or Policies	Frequency	Percentage
The privacy statement/policy is too long	146	78%
There is no point in reading the privacy statement/policy because I do not believe I can change any privacy settings	96	51%
The wording of the privacy statement/policy is difficult to understand	52	28%
I do not care how the company uses my data	29	15%
Other reasons for not always reading the privacy statement/policy	5	3%

Table 7. Respondents' Reactions to a Sample Data Usage and Privacy Statement (n = 204).

Perception of Data Usage and Privacy Statement	Frequency	Percentage
Indifferent	105	51%
Happy	39	19%
Concerned	36	18%
Safe	23	11%
Confused	12	6%
Surprised	7	3%
Other feelings	8	4%

Table 8. Respondents' Interpretations of a Sample Data Sharing Policy Statement (n = 204).

Perceptions of Data Sharing Policy Statement	Frequency	Percentage
Some information about me can be shared if personal identifiers, such as my name, have been removed	166	81%
My data may only be shared with those with whom I request it to be shared	34	17%
Any information about me, including my name, may be shared with third parties, such as advertisers	26	13%
Any data about me, including my name, may be shared with the public	21	10%
Other meaning	3	1%

Similarly, when presented with a data-sharing statement indicating that aggregated or de-identified information may be disclosed publicly or to third parties, 166 respondents (81%) understood it to mean that some information about them could still be shared once personal identifiers had been removed. However, 34 (17%) interpreted it to mean that data would only be shared with those they personally authorised, while 26 (13%) understood the statement to mean that any information about them, including their names, could be shared with third parties such as advertisers, and 21 (10%) interpreted it to mean that any data about them, including their names, could be shared with the public. These results suggest that not only awareness of formal laws, but also limited engagement with privacy statements and mixed interpretations of policy language in practice, impact respondents' governance-related legal and policy perceptions.

4.1.4. Demographic and Experiential Differences and Associations Across Governance-Related Factors

This section examines how the four governance-related factors included in the inferential analysis, namely general perceptions regarding WHD governance, trust regarding WHD, familiarity regarding WHD-related laws/acts, and perceptions of laws/acts regulating WHD, differ across gender, age, technological capability, and wearable use experience. It also presents the associations identified between wearable use experience and familiarity with WHD-related laws/acts, as well as perceptions of laws/acts regulating WHD. The tables showing the descriptive means and standard deviations for these governance-related factors across the demographic and experiential variables, as well as the inferential analysis results, are presented in Appendix A as Tables A1–A9.

As shown in Table A1, the descriptive mean scores were highest for trust regarding WHD (M = 3.50), followed by perceptions of laws and acts regulating WHD (M = 3.49), compared to general perceptions regarding WHD governance (M = 3.38). Familiarity with WHD-related laws and acts recorded the lowest mean score (M = 2.85). Across the demographic and experiential groups, the observed differences in mean scores were generally small for general perceptions regarding WHD governance and trust, but somewhat more noticeable for familiarity regarding laws/acts and perceptions of laws/acts regulating WHD.

Univariate ANOVA was then conducted to examine whether governance-related perceptions differed across gender, age, technological capability, and wearable use experience. The results showed no statistically significant differences in general perceptions of WHD governance across these variables. Similarly, no statistically significant effects were found for trust regarding WHD across the demographic and experiential variables, although age approached significance ($F(3, 190) = 2.49$, $p = 0.061$). These results suggest that core governance perceptions and trust were relatively stable across the demographic and experiential variables examined.

Significant differences emerged, however, in familiarity with WHD-related laws and acts. Familiarity with these laws and acts was higher among respondents aged 30–39 than among those in the younger group (aged 18–29), and it was also higher among respondents with high technological capability than among those with not-high capability. The differences are statistically significant for age, $F(3, 190) = 4.16$, $p = 0.007$, and technological capability, $F(1, 190) = 10.39$, $p = 0.001$, with the latter also showing moderate practical significance ($d = 0.60$). Post hoc analysis showed that respondents aged 30–39 reported higher familiarity with WHD-related laws and acts than those aged 18–29 (M = 3.20 versus M = 2.61, $p = 0.003$, $d = 0.68$), while respondents with high technological capability likewise reported higher familiarity than those with not-high capability (M = 3.08 versus M = 2.58, $p = 0.001$, $d = 0.60$). These results indicate that familiarity with WHD-related laws and acts varied meaningfully by age and digital capability.

Perceptions of laws and acts regulating WHD also differed significantly by age and by experience with using wearables. Age showed a statistically significant effect, $F(3, 190) = 3.36$, $p = 0.020$, and experience using wearables also showed a significant effect, $F(2, 190) = 4.20$, $p = 0.016$. Post hoc analysis showed that respondents aged 30–39 had significantly stronger perceptions of regulatory applicability than those above 50 (M = 3.88 versus M = 3.32, $p = 0.039$, $d = 0.60$). A significant difference also emerged between respondents with a satisfactory wearable use experience and those with a not-satisfactory experience (M = 3.67 versus M = 3.17, $p = 0.027$, $d = 0.62$). These results suggest that perceptions of regulatory fit were more sensitive to age and wearable use experience than broader governance perceptions or trust.

Chi-square analysis provided additional support for this pattern. Experience using wearables was significantly associated with familiarity with WHD-related laws and acts, $\chi^2(4, n = 204) = 23.27$, $p < 0.0005$, with a medium association (Cramér's $V = 0.24$). However, experience using wearables was not significantly associated with perceptions of laws regulating WHD, $\chi^2(4, n = 204) = 6.98$, $p = 0.137$. These association results indicate that the wearable use experience was more closely related to legal familiarity than to perceptions of regulatory applicability.

4.1.5. Relationships Among Governance-Related Factors

Correlation analysis among the four governance-related factors showed several meaningful relationships, as displayed in Table 9. General perceptions regarding WHD governance and trust regarding WHD were moderately and positively correlated ($r = 0.450$), indicating that respondents who reported stronger trust in WHD also tended to report more positive perceptions of WHD governance. Familiarity regarding WHD-related laws/acts and perceptions of laws/acts regulating WHD were also moderately and positively correlated ($r = 0.355$), suggesting that respondents who were more familiar with relevant laws and acts also tended to perceive those laws and acts as more applicable to regulating WHD.

Table 9. Pearson Correlations Among WHD Governance-Related Factors.

Factors/Variables	General Perceptions Regarding WHD Governance	Trust Regarding WHD	Familiarity Regarding WHD Related Laws/Acts	Laws/Acts Regulating WHD
General perceptions of WHD governance		**0.450**	−0.083	0.089
Trust regarding WHD	**0.450**		−0.031	**0.164**
Familiarity regarding WHD-related Laws/Acts	−0.083	−0.031		**0.355**
Laws/Acts regulating WHD	0.089	**0.164**	**0.355**	

Note: Values shown in red text indicate statistically and practically significant results. Bolded values represent statistically significant but not practically significant results.

A weaker positive correlation was observed between trust regarding WHD and perceptions of laws and acts regulating WHD ($r = 0.164$), indicating a slight tendency for stronger trust in WHD to coincide with more positive perceptions of the regulatory relevance of these laws and acts. The negative correlations between familiarity regarding WHD-related laws/acts and general perceptions regarding WHD governance ($r = -0.083$) and between familiarity regarding WHD-related laws/acts and trust regarding WHD ($r = -0.031$) were very weak and not statistically significant. Although the negative direction indicates a slight tendency for greater legal familiarity to coincide with lower general governance perceptions or trust, the small coefficients provide no evidence of a meaningful inverse relationship between these factors.

4.2. Qualitative Findings on Health Professionals' Perceptions of WHD Governance in South Africa

This subsection presents the qualitative findings on health professionals' perceptions of WHD governance in South Africa, beginning with the participant profile and followed by the three themes derived from the coded interview data. The data were coded into 10 codes and are presented in the subsequent sections under these themes, namely, Perceptions of Existing WHD Governance and Regulatory Adequacy, Governance Concerns in the Management and Use of WHD, and Proposed Governance Responses for WHD. The table containing the codes and complete corresponding quotes is presented in Appendix A as Table A10.

4.2.1. Participants Profile

The qualitative findings are based on interviews with six health professionals, identified by the unique codes HP1–HP6. The group comprised three females and three males, all with at least a first degree in Medicine and more than 10 years of professional experience. Their areas of practice included general practice and specialist fields such as cardiology, general surgery, family medicine, and chronic disease management. HP1, HP2 and HP3 are general practitioners with interests in chronic disease management, family medicine and primary healthcare. HP4, HP5, and HP6 are specialists in cardiovascular health and general surgery. These profiles collectively indicate that the perspectives reported in this paper are grounded in sustained clinical experience and professional engagement with health-related data.

4.2.2. Perceptions of Existing WHD Governance and Regulatory Adequacy

A prominent perspective that emerged from the qualitative data is the perceived inadequacy of, and uncertainty about, existing regulations in fully governing WHD, as expressed by all six participants. HP5 clearly reflects this uncertainty and perceived inadequacy, stating that:

> *"I'm not entirely sure about the specific regulations regarding wearables and their impact on the sensitivity and privacy of health data. While there are general data protection and privacy laws in place, it's unclear whether they fully address the unique challenges posed by wearable technology."*

Other participants' perspectives indicate a more explicit uncertainty, particularly regarding the POPI Act, where HP1 and HP3 expressed uncertainty about the Act's adequacy, as reflected in their quotes below.

> *"I don't know whether there are regulations available to ensure wearables do not play negative, disruptive roles, such as undermining the sensitivity and privacy of health data. I don't know of it. I didn't think that there were. The POPI Act doesn't do much unless there's somebody that you can nail, you see? Like a professional. But there are lots of people that don't even know what's going on"* (HP1)

> *"Wearable health data is not specifically covered by the POPI Act. Yeah, it is grey. Do I think there are regulations? I don't think there are regulations to ensure that wearables do not play negative, disruptive roles, like undermining the sensitivity and privacy of health data"*. (HP3)

Further reflecting the regulatory uncertainty based on the undefined nature of WHD, HP3 questioned whether WHD are considered personal health data and suggested that, in such a context, the POPI Act might provide coverage for sharing such data, stating that

> *"When it comes to data sharing of information. Yeah, I think the POPI Act is specific to wearable health data. Isn't your heart rate or personal information?"*. (HP3)

4.2.3. Governance Concerns in the Management and Use of WHD

The participants' accounts further show that regulatory uncertainty was closely tied to concerns about WHD sharing and security governance. Their reflections reveal that uncertainty extended beyond whether regulation exists to include how permissions for sharing are managed, how secure WHD remains once collected and transmitted, and how far such data may ultimately circulate. HP5 strongly reflects this concern, noting that:

> *"The proliferation of wearable devices and the data they generate also raises questions about how well this data is safeguarded and managed. Wearables often collect and transmit*

sensitive health information, and if not properly protected, this data can be vulnerable to breaches or unauthorised access."

Similarly, HP1 expressed uncertainty about the parameters and the scope of WHD sharing, stating, "*I don't really know how far wearable health data could go.*" In the face of such data-sharing uncertainty, there was also uncertainty about how unauthorised access could be prevented, as expressed by HP2, who stated that "*I am not sure what regulations are actually in place, and data can be breached very easily*." Moreover, there is concern that, even where patient-doctor agreements may guide WHD sharing, there remain practical and regulatory uncertainties, especially regarding permissions and how they are granted for data sharing. This view is clearly shared by HP3, who explained that:

"Yes, the patient-doctor service agreement already includes that. But also, sharing and access can be difficult because there are so many devices out there. . . .then they say, with the POPI Act, do we need permission, and how do they grant it on both sides for data sharing?"

Accessibility was also presented as a governance-related concern, both in terms of who may access WHD and the difficulty of retrieving and using such data in practice. On the one hand, HP6's reflections show concern that manufacturers and other actors within the data ecosystem may have more access to WHD than users initially realise. This is evident in HP6's expression of surprise and concern:

"I didn't think the manufacturers can see the data and access them, because it is their sensor that is collecting the data and the data is being stored in their storage facilities. So it means they can sell their data if they like. That can be a problem. "Can the manufacturers actually see the data? Oh, I never thought about the potential many third-party access and many people involved in the ecosystem of the data storage, eh."

On the other hand, HP3 highlighted the practical difficulty clinicians may face in accessing WHD across different devices, platforms, websites, and software requirements, especially in the absence of interoperability, stating that:

"A lot of people and companies say that it is easy to access, but it is never really easy to access. It could be a lot easier if you have someone dedicated in your practice to do that, but you as a doctor to now say, let's find a patient and let's download their data, makes it very difficult. So, at places like Intercare, where they do have a nurse, they do have someone who is dedicated to this, which makes it a lot easier, but for me, it's very difficult. But then you have to have the programme to enable direct access. So, now you have to have five different cables for five different machines. Or this website for that one, that one for this one. Instead of everyone integrating it. And now a patient comes to me, and I am like, what was the name of your machine again? Well, I don't remember which brand I have. And I'm like, now, which one of the five do I look at? They should all interlink. Should all interlink".

The commodification and monetisation of WHD in ways that do not primarily benefit the wearer also emerged as a concern requiring governance. HP2 raised this most directly, stating that:

". . .the companies that provide these things, specifically the watches, the Apple iWatch, and everything else. . . .as part of the vitality programme, they give you this watch for free. So they are able to collect your data. For marketing. For marketing and for restratifying the individual to whom the data is concerned. And to know how to adjust your premium. They are using the data for their own personal gain and not necessarily for the patient's well-being. And then surely they can use the data on their work analytics, or however they are using."

The perspective of HP2 reflects on how insurance companies may collect WHD through wearable-linked programmes and then commercialise the data for marketing, re-stratification, or premium adjustment. Related to this, participants also raised concerns about the impact that privacy risks may have on wearable users, particularly where data use may result in financial or other forms of disadvantage rather than patient benefit.

Trust in WHD remained qualified and defined by concerns about data quality, as the findings revealed, and this was a prominent point of reflection that emerged among almost all participants. For example, HP4 stated plainly that "*I do not trust the data collected through wearables as it concerns their reliability, validity and accuracy*," while HP6 similarly linked incomplete trust to the quality of the data, stating "*. . .I do not trust the data completely. No, I don't. I don't. The quality is why I do not completely trust the data from the wearables*." Furthermore, repeated doubts were raised about the reliability, validity, and accuracy of WHD, with HP6 describing the quality more broadly as "*still a concern*," and others indicating that many wearables are simply not very accurate. Specifically, HP5 stated that "*Although these devices can provide useful supplementary information, several concerns impact their trustworthiness. As a health professional, I am quite sceptical about the reliability, validity, and accuracy of data collected through wearables*." HP3 warned that it must be taken into consideration that "*not all of them are very accurate*", and HP4 similarly emphasised that "*The majority of them are inaccurate. It is a compromise of functionality and aesthetic/practicality*."

4.2.4. Proposed Governance Responses for WHD

Advocacy for stronger regulations and standards to govern WHD and address WHD management concerns emerged amid perceived inadequacies in existing regulations and uncertainty about whether they provide sufficient coverage for WHD governance. The advocacy was expressed most clearly by HP5, who stated that:

> *"There is a need for more robust regulations and standards to ensure that wearable health data meets high-quality standards and can be reliably used in clinical settings. In my opinion, wearables can pose risks to the sensitivity and privacy of health data. While they offer valuable insights and enhance health monitoring, they also introduce concerns about data security and patient privacy. Privacy and data security are also crucial concerns that need to be addressed to ensure that wearable health data are used responsibly. More detailed and targeted regulations might be needed to ensure comprehensive protection for health data collected by these devices. . . .strict data security and quality measures are vital to protect patient information and build trust in the use of these technologies".*

The findings further show that this advocacy extended beyond calls for stronger laws to include proposals for stakeholder collaboration in governing WHD, the classification of wearables as medical devices, and the standardisation of wearables and WHD as practical governance responses. For instance, pointing to collaboration between clinicians and technologists in setting and implementing quality standards, HP6 explained that:

> *"Regulating the quality of wearable health data might need technologists and health professionals working hand in hand. The doctors saying what the standard of quality health data should be in this regard and the technologists taking the recommendations and infusing it into the design. So, I think it's got to be regulated in the medical fraternity. So we as cardiologists and clinicians, will see the data and we will decide if it is accurate or not."*

HP3 advocated that, where appropriate, wearables should be classified and treated more like medical devices, so that they do not simply circulate without clear standards but instead fall under the recognised oversight and standardisation of the South African Health Products Regulatory Authority (SAHPRA). Subsequently, HP3 emphasised the possible

role of SAHPRA in regulating wearables through branding, explaining that wearables should have appropriate branding to show which of the devices can be integrated into health management and to encourage medical aid companies to support their use among clients. Their views are evident in the quote from their response below.

> *"...then they don't get to just sell them if they are classified as medical devices. So, have like a branding on the box that speaks to SAHPRA or relevant agency standardisation and regulation... one cannot just buy medical devices from anywhere, just as one cannot just buy any medication from anywhere. I do think this is clever because then we know what we can and can't use. Then, medical aids can start giving some money towards that."*

Overall, the participants' accounts from the interviews provide insights into governance-related perceptions pertaining to regulatory adequacy, WHD sharing and security, accessibility, commodification, trust, and quality, alongside proposals for stronger regulation, collaboration, classification, and standardisation.

5. Discussion

The perceptions of WHD governance in South Africa among wearable users and health professionals in the study were neither uniformly assured nor uniformly sceptical but rather reflected selective confidence, depending on the perspective from which it was viewed and who was viewing it. Thus, the overall perceptions reflected a governance environment regarded as relevant to the use and value of WHD across the two stakeholder groups, but not yet considered fully clear, established, or adequate. This recognition of governance relevance amid varying levels of confidence is an important insight because it establishes that perceptions of WHD governance do not rest on a single, clear judgment about whether governance is present or absent but instead reflect varying levels of confidence in its usability, protection, legal adequacy, and practical oversight.

5.1. Governance Perceptions Among Wearable Users

The perceptions of wearable users in the study regarding the accessibility, reliability, accuracy, sharing, and trustworthiness of WHD were generally favourable and more clearly formed, and these aspects are not experienced as major governance concerns in the practical use of WHD. These users perceive their WHD as generally accessible, reliable, accurate, shareable and relatively trustworthy. Similarly, privacy and third-party data practices appear to elicit positive perceptions, with relatively lower concern among these users, albeit less decisive and clearly formed confidence than was evident for access, trust, reliability, and accuracy. In essence, wearable users did not generally perceive the privacy of their WHD and the possibility of third-party analysis of these data as strongly concerning aspects of WHD governance, even though these perceptions were not as firmly established or widely shared. In contrast, security, the adequacy of current South African laws, and the need for additional regulations to govern WHD were perceived with greater uncertainty, indicating weaker confidence in the broader governance conditions surrounding WHD. Specifically, regarding WHD security, users did not generally perceive it as a strongly problematic aspect or as something to be outright distrusted, but neither did they express clear, firm confidence in its adequacy.

Positive perceptions are stronger where WHD governance is encountered and viewed through immediate use of the data and weaker where governance is hinged on or viewed through less visible legal, organisational, and technical safeguards. Governance appears to have been perceived more readily through the apparent functionality and availability of WHD than through informed confidence in the systems and rules that protect and regulate it. In practical terms, the positive wearable users' perceptions, therefore, should not be taken as evidence of a fully understood, trusted and established governance environment,

but rather as evidence that the benefits and usability of WHD were more readily perceived than the adequacy of its governance arrangements. For WHD governance to be strengthened in South Africa, governance efforts will need to address not only the availability and apparent usefulness of WHD but also the weaker areas of confidence surrounding protection, oversight, and regulatory adequacy.

This interpretation becomes even more valid and clearer in the relatively low level of privacy concern expressed by these users, yet their much greater uncertainty on whether manufacturers and their partners adequately secure WHD. The study by [91] similarly reported lower privacy concerns among wearable users. However, one must consider that upholding WHD privacy largely depends on the security measures that govern access. According to [69,92,93], upholding data privacy means that data is collected, processed, and shared in a manner that respects the rights of the data subject, supported by security measures such as anonymisation, pseudonymisation, and access control to protect data from unauthorised access, modification, or loss to avoid harming the owner. The ongoing collection of personal health data and its transmission through networks to third parties for storage and analysis can heighten wearable users' exposure to victimisation and misuse [94].

The privacy control of wearable users weakens when they are less able to determine the extent of access to WHD, as may be the case with remote, third-party storage architectures that are prone to inadequate security mechanisms. Thus, the insight that wearable users in the study are less concerned about privacy but not confident in the adequacy of their WHD security indicates that privacy may not always be understood in close relation to the technical and organisational conditions that sustain it. Instead, privacy may be perceived as a general expectation that data should not be misused, while security is treated as a more specialised or less visible aspect. The implication is that wearers' confidence in WHD governance may rest partly on incomplete understandings of how privacy compromises occur and how they are prevented. Cilliers [91] and Els and Cilliers [95] clarify this implication, stating that in most instances, wearable users are unaware of the storage mechanisms adopted by their wearable manufacturers and only trust that appropriate regulations are in place and followed to ensure secure storage and, consequently, the privacy compliance of their data. Hence, a possible gap exists between governance confidence and governance understanding, and it is not simply a matter of wearable users' indifference to privacy. Given the study's focus on governance, this insight matters because it points to a practical starting point for strengthening WHD governance in South Africa, where governance improvement may need to begin with greater awareness and governance literacy regarding how privacy is actually protected, compromised, and managed. In that sense, wearers' roles in governance cannot be limited to being data subjects only, but they also need some understanding of permissions, access conditions, sharing implications, and the safeguards that underpin responsible WHD use. Without such foundational understanding, confidence in governance may remain partial and fragile, even where WHD use itself is viewed positively.

The POPI Act is the law most strongly associated with WHD regulation, yet this did not translate into equivalent confidence that current regulations in South Africa are adequate for protecting WHD privacy. Wearable users generally recognise that WHD is associated with risks that require stronger safeguards, yet they perceive the available governance regulatory frameworks as partial and inadequate, with calls for more adequate regulation to be in place in South Africa. The key insight here is that legal familiarity and legal assurance are not the same. Wearable users may recognise the POPI Act as the most visible and relevant law in the data protection environment, while still remaining uncertain about whether it sufficiently addresses the distinctive realities of WHD, including

continuous generation, platform dependence, multi-actor access, and wearable-specific privacy risks. Moreover, the uneven familiarity of wearable users with other existing laws, together with the widespread undecided stance on legal adequacy, suggests that the regulatory environment is perceived more as a general framework than as a clearly understood system of governance specifically tailored to WHD. In this sense, the visibility of existing governance instruments appears to have outpaced their clarity on relevance and fitness for purpose.

Limited clarity in existing governance regulations is also reflected in how wearable users engaged with privacy policy statements and in their interpretations of the language used. The fact that many did not read privacy statements, or did so only inconsistently, while also viewing them as overly long, difficult to understand, or practically unhelpful, suggests that formal governance communication was not serving as an effective basis for governance understanding. Similarly, their interpretations of the provided sample data usage and sharing statements point in the same direction. Indifference to the usage statement and mixed interpretations of the data-sharing statement indicate that the governance implications of data processing, disclosure, and de-identification were not always clearly understood. This insight is important because it suggests that wearable users' perceptions of WHD governance were actively informed and shaped not only by the visibility and awareness of governance instruments, but also by weak engagement with the very policy texts meant to communicate data governance practices. Similar reports exist in the literature on the unfamiliarity with the WHD privacy protection policies among users [91], the complexity of the language used in these policies [96] and the lack of user agency and autonomy in WHD privacy protection [97].

In this regard, perceptions of governance among wearable users seem to rest partly on a fragile informational base, in which familiarity with policy statements or their terminology does not necessarily translate into a clear understanding of what those statements permit or protect. For effective WHD governance, the implications of such inadequately formed perceptions are that informed consent, which is one way of ensuring privacy, can no longer be said to be effective if wearable users are truly not informed or capacitated to make informed decisions about consent. Indications from [1,49,98,99], show that, as a mechanism for ensuring privacy, consent must be informed; otherwise, privacy violations become imminent. Similarly, Ref. [96], beyond describing the language of privacy statements as complex, opined that most privacy statements for IoTs are generic and often lack adequate information to provide assurance of privacy protection. According to [1], wearable users expect wearable manufacturers and their partners to provide clear, easy-to-read privacy policies to better support informed consent, although this expectation remains elusive in practice. In practice, wearable users may be pressured, persuaded, or effectively compelled to give up privacy rights in exchange for personalised wearable services [97]. The legitimacy of consent as a privacy mechanism is undermined if users cannot adequately interpret or evaluate the meaning of related policy statements, and the consent provided therefore risks being symbolic rather than substantive.

A further look at how perceptions are formed and differ among wearable users reveals that general impressions of WHD governance may be more easily shared across wearable user groups than the more specific legal and regulatory dimensions of governance perception. General perceptions of governance and trust are relatively similar across gender, age, technological capability, and wearable use experience. However, familiarity with WHD-related laws and perceptions of laws regulating WHD vary by age, technological capability, and wearable use experience. Put differently, broad confidence in WHD and more precise awareness of regulations and their relevance do not appear to operate in the same way. General governance sentiment may be informed by everyday use and

perceived value, whereas regulatory familiarity and perceptions of regulatory fit depend more on experience, capability, and exposure. Understanding this distinction is important because it shows that explicating perceptions of governance requires attention to both broad evaluative sentiment and specific awareness of governance and regulatory instruments, rather than assuming that one naturally implies the other. This broader differentiation in how perceptions are formed aligns with [45] view that privacy and governance-related perceptions around wearables are context-dependent and shaped by a range of personal and technological factors.

5.2. WHD Governance Perception Among Health Professionals

The perceptions of WHD governance among health professionals in the study bring an important dimension to understanding WHD governance in South Africa, albeit in contrast to those expressed by wearable users. However, the point here is not primarily one of mere comparison but to adequately understand how perceptions are formed, the different dimensions that may exist, and the implications for effective WHD governance, ensuring that multiple perspectives and views are recognised in working towards it.

Health professionals were more cautious in their perceptions and placed greater emphasis on regulatory adequacy, data quality, security, and oversight. Their accounts suggest that WHD governance is viewed not simply as underdeveloped in a regulatory sense, but as uncertain in the practical and professional conditions required for WHD to be meaningfully used in health-related contexts, especially clinical settings. Godfrey et al. [2] convey a similar sense of restraint, cautioning that although wearables may support innovative approaches to patient treatment and management, their growing use in healthcare also exposes users and clinicians to devices that may lack robust design, pragmatic utility, patient or clinician engagement, and, importantly, adequate validation or verification. Unlike wearable users, whose governance perceptions were more often informed by perceived everyday value of the WHD, health professionals emphasised the governance conditions under which such data would need to be shared, secured, interpreted, trusted, and potentially integrated into care. Their concerns, therefore, extended beyond whether WHD is available or useful and centred more on whether it is governed in a manner consistent with quality, accountability, and safe use. Similar concerns are indicated by [2], who note that the deployment of wearables in clinical settings remains contentious, partly because it is often unclear what governance regulatory framework applies and whether such devices fall within medical device regulatory frameworks, while no clear regulatory requirements exist for robust capture, quantification, validation, or verification of many of their generated health data or outputs. The difference in standpoints between health professionals and wearable users in this study is a significant insight, as it shows that perceptions of governance vary not only by attitude but also by the purpose for which WHD is being imagined.

One of the clearest contributions of the health professionals' accounts is their connection of governance to quality and trust. Their repeated concern with reliability, validity, and accuracy indicates that trust in WHD was not treated as an abstract disposition but as contingent on whether the data could be regarded as dependable for clinical purposes and other health routine management. This concern closely mirrors the observation in [2] that wearables adopted in healthcare may bypass robust validation and verification procedures, typically conducted through clinical trials, even though these procedures are essential for determining whether devices perform as intended for relevant stakeholders. In this regard, the health professionals' caution in the present study reflects a wider concern that trust in WHD cannot be separated from the extent to which the devices and their outputs have been transparently and rigorously assessed. Moreover, when the health professionals' cautious

perceptions are considered alongside the more favourable and unguarded trust perceptions among wearable users, it implies that trust in WHD is not uniform across stakeholder groups because the standards against which it is assessed differ. For wearable users, trust may reflect confidence that the data are personally useful, plausible, or sufficiently consistent for everyday purposes. For health professionals, trust is more conditional and closely tied to whether WHD meets the quality thresholds required for clinical reliance. In that sense, the indication is that trust and quality are inseparable from the clinical perspective of WHD governance. Trust is not simply about believing the data; it is about whether the quality of the data is adequately governed to be fit for purpose.

Furthermore, the health professionals' perceptions of WHD governance raise concerns about sharing, security, access, commodification, and monetisation, thereby broadening the cautious view of governance. Such concern reflecting perceptions implies that governance is not only about protecting WHD from breach or unauthorised access, but also about managing the broader data ecosystem within which WHD moves and accumulates value. Questions raised by health professionals about who can access the data, how permissions are granted, how fragmented systems hinder retrieval, and how data may be used for marketing, profiling, or premium adjustments all point to governance as a matter of authority, accountability, purpose, and benefit, not only privacy. These concerns also align with Sankin's [79] observation that wearable manufacturers and their partners may treat WHD as a lucrative commodity, whether through selling advertising access, trading personal health data, or advancing analytics capabilities for profit, thereby reinforcing the governance importance of questions of benefit, control, and accountability.

According to the health professionals, privacy risks are associated with potential financial or other disadvantages for wearable users when adequate governance is not in place in programmes presented by health insurance providers as beneficial for promoting healthy lifestyles. In this regard, such practices may expose wearers to harm, such as the misuse of their health data to adjust health insurance premiums or policies on the basis of pre-existing medical conditions [94]. These concerns, as reflected in the health professionals' perceptions, resonate with global critiques of the commodification of personal behavioural data, treated as tradable assets in what Zuboff [100] termed "surveillance capitalism". Similar concerns have also been raised in the South African context regarding the commercialisation of health data from digital health technologies, with a warning that if left unregulated, it risks undermining public trust in digital health innovations [101]. Specifically pertaining to WHD, Refs. [97,99,102,103] all criticised the practice of selling WHD to third parties for financial gain without the consent of wearable users. These concerns are particularly significant in a context such as South Africa, where access to formal healthcare and insurance remains socially and economically stratified [16]. The discussion, therefore, points beyond a narrow protection model towards a broader account of governance in which control over data flows, the purposes of data use, and the prevention of exploitative or asymmetrical benefit become central.

The health professionals' perceptions of WHD governance in South Africa extended beyond identifying gaps or risks to also encompass what stronger governance might entail to effectively respond to them. The emphasis on, and recommendation for, more robust regulation and standards, collaboration between health professionals and technologists, classification of wearables as medical devices where appropriate, SAHPRA-linked oversight, standardisation, and stricter data security and quality measures indicate that governance was also imagined in practical and institutional terms. Such emphasis and recommendations are important to avoid situations that [2] warned about in which healthcare professionals rely on WHD and wearable outputs that "conceal hidden barriers to robust patient assessment" because they lack sufficient transparency, validation, or verification

for health-related use. The health professionals' perceptions were not simply critical, but constructive, pointing to a governance model that would do more than protect WHD as an abstract function. Such an envisaged governance model would also clarify responsibility, improve data quality expectations, strengthen oversight, and support greater confidence in the use of WHD within health-related contexts, especially clinical settings. In this respect, the health professionals' accounts help move the discussion from what is perceived as lacking towards what can be regarded as practical pathways for improving WHD governance, as well as what governance would need to provide in order to be regarded as adequate. Strengthening WHD governance in South Africa will likely require a combination of clearer legal articulation, stronger standardisation, quality-focused oversight, and more coordinated institutional roles. Theoretically, this interpretation supports the view that governance is not perceived only as a legal framework, but as a broader arrangement of oversight, responsibility, standards, and operational safeguards [72–74,104–107]. In practical terms, it implies that the efficient and sustained use of WHD in health management will depend on governance efforts that are visible enough for wearers to understand, robust enough for health professionals to trust, and coordinated enough to manage quality, access, security, and accountability in tandem.

6. Limitations of the Study

The study that underpins this paper is not without limitations that warrant caution when interpreting the generalisability of its findings. The quantitative component was limited to wearable users and therefore reflects only the perceptions of a sample of those already engaged with wearable use at the time of the study's data collection. Similarly, the use of voluntary sampling may introduce self-selection bias because participation depends on individuals' willingness to respond, and the resulting sample may not be statistically representative of all wearable users in South Africa.

The qualitative component, while valuable for adding professional insight, was limited to six practising medical doctors purposively selected for their professional experience and relevant engagement with WHD and health data in practice. Although the sample was sufficient for obtaining the in-depth professional perspectives required for this component, its size and composition limit the breadth of health professional perspectives represented, and it is not intended to be statistically representative. The findings should therefore not be regarded as representative of the WHD governance perceptions of health professionals in South Africa generally, particularly among other health professional groups and in clinical settings not included in the study. These limitations affect the scope and generalisability of the findings but do not detract from the study's contribution or diminish its value within the context and stakeholder groups investigated. The findings should therefore be understood as providing contextual, specific, key stakeholder-based insight rather than a comprehensive representation of WHD governance perceptions across all stakeholders and settings in South Africa.

7. Conclusions

The perceptions of WHD governance among wearable users and health professionals in South Africa are significant not only because they reveal where confidence and concern lie, but also because they point to what must be addressed if WHD governance is to be meaningfully strengthened. This paper contributes to understanding WHD governance in South Africa by showing that governance is perceived not only through formal regulation but also through the everyday conditions under which WHD is accessed, interpreted, trusted, protected, and used. Its main contribution lies in demonstrating that perceptions of WHD governance are stakeholder-dependent and reveal different governance priorities.

For wearable users, the key issue is not simply whether governance exists, but whether it is sufficiently intelligible to support informed and confident use of WHD. For health professionals, the issue extends further to whether governance is credible enough to support quality, accountability, and meaningful use of WHD in health management.

In explicating the perceptions of WHD governance among the studied key stakeholders, the paper further demonstrates that WHD governance is understood not only as a matter of law, policy or regulatory framework, but also through access, usability, trust, quality, control, and the practical conditions under which WHD circulates and becomes valuable. In this sense, the paper establishes that governance of WHD is perceived as necessary by these stakeholders but differently experienced, weighted, and judged according to their position in relation to the data. These insights also highlight what matters for advancing WHD governance in practice.

The practical implication is that WHD governance in South Africa cannot be strengthened solely through regulation in principle, and this understanding is highly relevant to WHD governance role-players in the country. WHD governance role-players must consider WHD governance as both a legal and a socio-technical matter, requiring not only rules and protections but also awareness, credibility, and workable oversight. More is required in the form of clearer legal communication, stronger governance literacy among wearable users, better alignment between privacy protection and security practices, and governance arrangements that are practical to health professionals in responding to issues of data quality, interoperability, access, security and accountability. Thus, sustaining the effective use of WHD in health management will depend on governance arrangements that are visible enough for users to understand and robust enough for health professionals to trust.

The paper also contributes theoretically by showing that perceptions of WHD governance are not reducible to a single judgement of confidence or concern. Instead, they are formed through different encounters with WHD and different expectations of what governance should provide. This supports an understanding of governance as a broader arrangement of rules, responsibilities, standards, safeguards, and practical oversight, rather than as law or compliance alone.

Future research can build on this study in several ways. There is scope for more focused work on governance literacy among wearable users, particularly regarding privacy, security, and the application of the relevant regulatory framework to WHD. Further research could also investigate the practical implementation of governance arrangements by manufacturers, health insurers, technology policymakers, data regulators, and healthcare institutions. Future studies could also include a larger and more diverse range of health professionals and healthcare settings to examine whether similar governance perceptions are evident across professional groups and contexts. More work is also needed on data quality, interoperability, accountability, and the forms of governance most likely to support trustworthy and sustainable use of WHD in health management. In addition, comparative work across broader stakeholder groups and contexts would help clarify how WHD governance expectations differ and what forms of governance are most likely to support trustworthy, quality-oriented, and sustainable use of WHD in health management.

Author Contributions: Conceptualisation, L.O.I., I.F. and B.S.; methodology, L.O.I.; software, L.O.I.; validation, L.O.I., I.F. and B.S.; formal analysis, L.O.I.; investigation, L.O.I.; resources, L.O.I., I.F. and B.S.; data curation, L.O.I.; writing—original draft preparation, L.O.I.; writing—review and editing, L.O.I., I.F. and B.S.; visualisation, L.O.I.; supervision, B.S. and I.F.; project administration, L.O.I.; funding acquisition, L.O.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Research Foundation (NRF) of South Africa (Grant number: PMDS22061321709), the Postgraduate Research Scholarship (PGRS) at Nelson Mandela University, and the Telkom Centre of Excellence (CoE) at Nelson Mandela University.

Institutional Review Board Statement: The study on which this paper is based was conducted in accordance with the Declaration of Helsinki and approved by the Research Ethics Committee—Human (REC-H) at Nelson Mandela University. The ethics approval number is 2023-SCI-0233, and the approval date was 20 October 2023.

Informed Consent Statement: Informed consent was obtained from all individuals (participants and respondents) involved in the study.

Data Availability Statement: The data supporting the findings of this study are not publicly available due to privacy and ethical restrictions but may be available from the corresponding author upon reasonable request, within associated ethical restrictions and subject to applicable ethical approval and confidentiality requirements.

Acknowledgments: AI tools (ChatGPT—GPT-5) were used for language refinement, grammar checking and general editorial support during manuscript preparation. The authors reviewed, verified, and take full responsibility for the final content.

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

Appendix A. Inferential Analysis Results Tables and Qualitative Data Table

Appendix A contains the 10 supplementary tables referenced and reported on in the paper but not presented, which support the quantitative and qualitative findings. These include the inferential analysis results tables and the qualitative data table showing the codes and corresponding example quotes from the health professionals' interviews.

Table A1. Demographic Variables and WHD Governance Perceptions Factors for the ANOVA.

Groups	Level		General Perceptions Regarding WHD Governance	Trust Regarding WHD	Familiarity Regarding WHD-Related Laws/Acts	Laws/Acts Regulating WHD
		n	Mean	Mean	Mean	Mean
		Percentage	SD	SD	SD	SD
Total		198	3.38	3.50	2.85	3.49
		100%	0.49	0.60	0.86	0.96
Gender	Female	128	3.39	3.52	2.87	3.53
		65%	0.48	0.60	0.86	0.93
	Male	70	3.36	3.45	2.83	3.44
		35%	0.53	0.59	0.85	1.02
Age	18–29	70	3.46	3.65	2.61	3.46
		35%	0.50	0.57	0.85	0.79
	30–39	45	3.35	3.43	3.20	3.88
		23%	0.50	0.68	0.88	0.80
	40–49	33	3.26	3.38	2.83	3.32
		17%	0.44	0.38	0.89	1.23
	Above 50	50	3.36	3.42	2.90	3.32
		25%	0.52	0.65	0.73	1.05

Table A1. *Cont.*

Groups	Level		General Perceptions Regarding WHD Governance	Trust Regarding WHD	Familiarity Regarding WHD-Related Laws/Acts	Laws/Acts Regulating WHD
Capability using digital technologies in general	Not high-level	89	3.32	3.41	2.58	3.41
		45%	0.48	0.56	0.78	0.94
	High level	109	3.43	3.57	3.08	3.57
		55%	0.50	0.62	0.85	0.98
Experience using wearables	Satisfactory	86	3.36	3.48	2.81	3.67
		43%	0.46	0.55	0.80	0.77

Note: ANOVA results are based on complete cases only (n = 198).

Table A2. Univariate ANOVA Results for General Perceptions Regarding WHD Governance (n = 198).

Demographic Variables	*F*-Value	*df*	*p*	Cohen's *d*
Gender	0.10	1, 190	0.747	n/a
Age	1.53	3, 190	0.209	n/a
Capability using digital technologies in general	0.36	1, 190	0.549	n/a
Experience using wearables	1.70	2, 190	0.185	n/a

Table A3. Univariate ANOVA Results for Trust Regarding WHD (n = 198).

Demographic Variables	*F*-Value	*df*	*p*	Cohen's *d*
Gender	0.50	1, 190	0.480	n/a
Age	2.49	3, 190	0.061	n/a
Capability using digital technologies in general	1.50	1, 190	0.222	n/a
Experience using wearables	0.96	2, 190	0.383	n/a

Table A4. Univariate ANOVA Results for Familiarity Regarding WHD-related Laws/Acts (n = 198).

Demographic Variables	*F*-Value	*df*	*p*	Cohen's *d*
Gender	1.50	1, 190	0.222	n/a
Age	4.16	3, 190	0.007	n/a
Capability using digital technologies in general	10.39	1, 190	0.001	0.60
Experience using wearables	2.17	2, 190	0.117	n/a

Note: Values shown in red text indicate statistically significant results.

Table A5. Post Hoc Results for Familiarity Regarding WHD-related Laws/Acts (n = 198).

Demographic Variables	Level 1	Level 2	M_1	M_2	*p*	Cohen's *d*
Age	18–29	30–39	2.61	3.20	0.003	0.68
	18–29	40–49	2.61	2.83	0.639	0.25
	18–29	Above 50	2.61	2.90	0.271	0.37
	30–39	40–49	3.20	2.83	0.264	0.41
	30–39	Above 50	3.20	2.90	0.368	0.36
	40–49	Above 50	2.83	2.90	0.982	0.09
Capability using digital technologies in general	Not high level	High level	2.58	3.08	0.001	0.60

Note: Values shown in red text indicate statistically significant results.

Table A6. Univariate ANOVA Results for Laws/Acts Regulating WHD (n = 198).

Demographic Variables	*F*-Value	*df*	*p*	Cohen's *d*
Gender	0.46	1, 190	0.498	n/a
Age	3.36	3, 190	0.020	n/a
Capability using digital technologies in general	0.81	1, 190	0.369	n/a
Experience using wearables	4.20	2, 190	0.016	n/a

Note: Values shown in red text indicate statistically significant results.

Table A7. Post Hoc Results for Laws/Acts Regulating WHD (n = 198).

Demographic Variables	Level 1	Level 2	M_1	M_2	*p*	Cohen's *d*
Age	18–29	30–39	3.46	3.88	0.136	0.53
	18–29	40–49	3.46	3.32	0.915	0.15
	18–29	Above 50	3.46	3.32	0.890	0.15
	30–39	40–49	3.88	3.32	0.076	0.56
	30–39	Above 50	3.88	3.32	0.039	0.60
	40–49	Above 50	3.32	3.32	1.000	0.00
Experience using wearables	Satisfactory	Not satisfactory	3.67	3.17	0.027	0.62
	Satisfactory	High	3.67	3.45	0.338	0.23
	Not satisfactory	High	3.17	3.45	0.320	0.27

Note: Values shown in red text indicate statistically significant results.

Table A8. Experience Using Wearables by Familiarity with WHD-Related Laws/Acts (n = 204).

Familiarity with WHD-Related Laws/Acts	Experience Using Wearables							
	Not Satisfactory		Satisfactory		High		Total	
Lower (≤Q1)	20	35%	27	47%	10	18%	57	100%
Middle (Q1–Q3)	12	11%	47	43%	50	46%	109	100%
Higher (>Q3)	4	11%	15	39%	19	50%	38	100%
Total	36	17.7%	89	43.6%	79	38.7%	204	100%
$Chi^2(df = 4, n = 204) = 23.27; p < 0.0005; V = 0.24$ Medium								

Note: Chi-square results are based on the full valid sample for the variables included (n = 204).

Table A9. Experience Using Wearables by Perceptions of Laws/Acts Regulating WHD (n-204).

Laws/Acts Regulating WHD	Experience Using Wearables							
	Not Satisfactory		Satisfactory		High		Total	
Lower (<Q1)	9	26%	13	37%	13	37%	35	100%
Middle (Q1–Q3)	22	21%	44	42%	38	37%	104	100%
Higher (≥Q3)	5	8%	32	49%	28	43%	65	100%
Total	36	17.7%	89	43.6%	79	38.7%	204	100%
$Chi^2(df = 4, n = 204) = 6.98; p = 0.137$								

Table A10. Health professionals' perceptions of WHD governance.

Code and Description	Example Quote
Regulatory importance and need: Captures perspectives on the need for stronger regulation and standards for WHD, especially for clinical reliability and use.	**HP5**: "*There is a need for more robust regulations and standards to ensure that wearable health data meets high-quality standards and can be reliably used in clinical settings. In my opinion, wearables can pose risks to the sensitivity and privacy of health data. While they offer valuable insights and enhance health monitoring, they also introduce concerns about data security and patient privacy. Privacy and data security are also crucial concerns that need to be addressed to ensure that wearable health data are used responsibly. More detailed and targeted regulations might be needed to ensure comprehensive protection for health data collected by these devices.*"
Perceived governance regulation adequacy: Captures the view on whether existing legal frameworks may address the distinctive governance challenges of WHD.	**HP5**: "*I'm not entirely sure about the specific regulations regarding wearables and their impact on the sensitivity and privacy of health data. While there are general data protection and privacy laws in place, it's unclear whether they fully address the unique challenges posed by wearable technology.*" **HP1**: "*I don't know whether there are regulations available to ensure wearables do not play negative, disruptive roles, such as undermining the sensitivity and privacy of health data. I don't know of it. I didn't think that there were. The POPI Act doesn't do much unless there's somebody that you can nail, you see? Like a professional. But there are lots of people that don't even know what's going on.*" **HP4**: "*I don't know if there are regulations available to ensure wearables do not play negative disruptive roles, such as undermining the sensitivity and privacy of health data. It wouldn't really concern a clinician. Its more on a policy or protocol level.*" **HP6**: "*I am not aware that there are regulations available to ensure wearables does not playing negative roles, but I'm sure, it should be. I was not aware that there are these regulations available.*" **HP3**: "*When it comes to data sharing of information. Yeah, I think the POPI Act is specific to wearable health data. Isn't your heart rate or personal information? Wearable health data is not specifically covered by the POPI Act. Yeah, it is grey. Do I think there are regulations? I don't think there are regulations to ensure that wearables do not play negative, disruptive roles, like undermining the sensitivity and privacy of health data*" **HP2**: "*I am not sure what regulations are actually in place, and data can be breached very easily.*"
Stakeholders' governance collaboration: Captures the perceived need for collaboration between clinicians and technologists in governing WHD.	**HP6**: "*Yes, definitely, regulating the quality of wearable health data might need technologists and health professionals working hand in hand. The doctors saying what the standard of quality health data should be in this regard and the technologists taking the recommendations and infusing it into the design. So, I think it's got to be regulated in the medical fraternity. So we as cardiologists and clinicians, will see the data and we will decide if it is accurate or not.*"
SAHPRA's governance role: Captures perspectives on the possible role of SAHPRA where wearables function as medical devices.	**HP3**: "*Yeah, then they don't get to just sell them if they are classified as medical devices. So, have like a branding on the box that speaks to SAHPRA or relevant agency standardisation and regulation. Exactly, one cannot just buy medical devices from anywhere just as one cannot just buy any medication from anywhere. I do think this is clever because then we know what we can and can't use. Exactly, yeah. Then, medical aids can start giving some money towards that.*"
Sharing and Security Governance: Captures perspectives on WHD sharing and security governance and regulation.	**HP3**: "*Yes, the patient-doctor service agreement already includes that. But also sharing and access can be difficult because there are so many devices out there. . . .then they say, with the POPI Act, do we need permission, and how do they grant it on both sides for data sharing?*" **HP1**: "*I don't really know how far wearable health data could go.*" **HP5**: "*Wearables often collect and transmit sensitive health information, and if not properly protected, this data can be vulnerable to breaches or unauthorised access. The proliferation of wearable devices and the data they generate also raises questions about how well this data is safeguarded and managed. Ensuring that wearable health data is secure, and that patient privacy is protected is a significant concern. There must be robust measures in place to safeguard sensitive health information. Strict data security measures are vital to protect patient information and build trust in the use of these technologies.*" **HP2**: "*I am not sure what regulations are actually in place, and data can be breached very easily.*"
Data Commodification and Monetisation: Captures concerns about the commercialisation of WHD and whether this data is being monetised without wearers' consent.	**HP2**: "*. . .the companies that provide these things, specifically the watches, the Apple iWatch, and everything else. . . .as part of the vitality programme, they give you this watch for free. So they are able to collect your data. For marketing. For marketing and for restratifying the individual to whom the data is concerned. And to know how to adjust your premium. They are using the data for their own personal gain and not necessarily for the patient's well-being. And then surely they can use the data on their work analytics, or however they are using. "*

Table A10. *Cont.*

Code and Description	Example Quote
Accessibility Perceptions: Captures how WHD access is generally perceived as a concern and how it is experienced.	**HP6**: "*I didn't think the manufacturers can see the data and access them, because it is their sensor that is collecting the data and the data is being stored in their storage facilities. So it means they can sell their data if they like. That can be a problem*" **HP6**: "*Can the manufacturers actually see the data? Oh, I never thought about the potential many third-party access and many people involved in the ecosystem of the data storage, eh.*" **HP5**: "*. . .this data can be vulnerable to breaches or unauthorised access.*" **HP3**: "*. . .a lot of people and companies say that it is easy to access, but it is never really easy to access. It could be a lot easier if you have someone dedicated in your practice to do that, but you as a doctor to now say, let's find a patient and let's download their data, makes it very difficult. So, at places like Intercare, where they do have a nurse, they do have someone who is dedicated to this, which makes it a lot easier, but for me, it's very difficult. But then you have to have the programme to enable direct access. So, now you have to have five different cables for five different machines. Or this website for that one, that one for this one. Instead of everyone integrating it. And now a patient comes to me, and I am like, what was the name of your machine again? Well, I don't remember which brand I have. And I'm like, now, which one of the five do I look at? They should all interlink. Should all interlink*"
Trust in WHD: Captures the perception and concerns about the confidence in and trustworthiness of WHD for clinical or personal use.	**HP4**: "*No, I do not trust the data collected through wearables as it concerns their reliability, validity and accuracy.*" **HP6**: "*Do I trust the quality of data from wearables? I do not trust the data completely. No, I don't. I don't. The quality is why I do not completely trust the data from the wearables.*" **HP5**: "*Although these devices can provide useful supplementary information, several concerns impact their trustworthiness.*"
Quality Perception: Captures how participants generally perceive the quality of WHD as a concern.	**HP5**: "*As a health professional, I am quite sceptical about the reliability, validity, and accuracy of data collected through wearables.*" **HP6**: "*The quality of data is still a concern*" **HP3**: *The thing that I think needs to be taken into consideration is not all of them are very accurate*" **HP4**: "*The majority of them are inaccurate. It is a compromise of functionality and aesthetic/practicality.*"
Privacy risk Impact: Captures concerns about how privacy risks in WHD management can have negative consequences for users.	**HP2**: "*. . .on a financial aspect, more to the patient than anything else because the companies that provide these things, specifically the watches, the Apple, iWatch, and everything else. They are using the data for* their own *personal gain and not necessarily for the patient's well-being.*" **HP2**: "*For the privacy of wearable health data, I have concerns about how the insurance companies are using this data. Yeah, because I come from the insurance industry. In the past, and this is how discovery is light years ahead because they, as part of the vitality programme, give you this watch for free. So they are able to collect your data for marketing and for restratifying the individual to whom the data is concerned. And to know how to adjust your premium. And I'm sure Discovery is doing that. I don't know if they are really doing, but what are they doing with these things [data]? If you are reaching your vitality points with your exercise activity and your movement, with your steps or whatever, then surely they are collecting your data. And then surely they can use the data on their work analytics, or however they are using. Because else they wouldn't offer you that product at a low cost. I think that is a concern.*"

References

1. Segura Anaya, L.H.; Alsadoon, A.; Costadopoulos, N.; Prasad, P.W.C. Ethical implications of user perceptions of wearable devices. *Sci. Eng. Ethics* **2018**, *24*, 1–28. [CrossRef]
2. Godfrey, A.; Hetherington, V.; Shum, H.; Bonato, P.; Lovell, N.H.; Stuart, S. From A to Z: Wearable technology explained. *Maturitas* **2018**, *113*, 40–47. [CrossRef]
3. Mashhadi, A.; Kawsar, F.; Acer, U.G. Human data interaction in IoT: The ownership aspect. In Proceedings of the 2014 IEEE World Forum on Internet of Things, Seoul, Republic of Korea, 6–8 March 2014; pp. 159–162. [CrossRef]
4. Schumann, M.; Doherty, C. Bridging gaps in wearable technology for exercise and health professionals: A brief review. *Int. J. Sports Med.* **2024**, *45*, 949–957. [CrossRef]
5. Watt, A.; Swainston, K.; Wilson, G. Health professionals' attitudes to patients' use of wearable technology. *Digit. Health* **2019**, *5*, 2055207619845544. [CrossRef]
6. Ghadi, Y.Y.; Shah, S.F.; Waheed, W.; Mazhar, T.; Ahmad, W.; Saeed, M.M.; Hamam, H. Integration of wearable technology and artificial intelligence in digital health for remote patient care. *J. Cloud Comput.* **2025**, *14*, 39. [CrossRef]
7. Sun, Y.; Chen, J.; Ji, M.; Li, X. Wearable technologies for health promotion and disease prevention in older adults: Systematic scoping review and evidence map. *J. Med. Internet Res.* **2025**, *27*, e69077. [CrossRef]

8. Alaboud, K.; Shahreen, M.; Islam, H.; Paul, T.; Zaman Rana, M.K.; Morrison, A.; Kumar, A.; Mohammad Mosa, A.S. Clinicians' perspectives in using patient-generated health data to improve ischemic heart disease management. *AMIA Summits Transl. Sci. Proc.* **2022**, *2022*, 112–119.
9. Alsabah, M.; Naser, M.A.; Albahri, A.S.; Albahri, O.S.; Alamoodi, A.H.; Abdulhussain, S.H.; Alzubaidi, L. A comprehensive review on key technologies toward smart healthcare systems based IoT: Technical aspects, challenges and future directions. *Artif. Intell. Rev.* **2025**, *58*, 343. [CrossRef]
10. Hu, S.; Song, D.; Wan, S.; Zhang, S.; Luo, C.; Li, N.; Liu, G.; Graça Espírito Santo Vasconcelos, J.; de Carvalho, L.L.C.; Neobísi, E.; et al. Digital health: Current applications, challenges, and future directions for enhancing healthcare quality and safety. *Front. Public Health* **2025**, *13*, 1646802. [CrossRef]
11. World Health Organization (WHO). *Global Strategy on Digital Health 2020–2025*; WHO: Geneva, Switzerland, 2021. Available online: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf (accessed on 24 April 2026).
12. Shajari, S.; Kuruvinashetti, K.; Komeili, A.; Sundararaj, U. The emergence of AI-based wearable sensors for digital health technology: A review. *Sensors* **2023**, *23*, 9498. [CrossRef]
13. Suryaprabha, T.; Choi, C.; Wu, Y.; Liu, L.; Hwang, B. Smart wearable and implantable biosensors for continuous health monitoring: Materials, biocompatibility, and AI integration. *npj Flex. Electron.* **2026**, *10*, 46. [CrossRef]
14. Arokiasamy, P.; Uttamacharya; Kowal, P.; Capistrant, B.D.; Gildner, T.E.; Thiele, E.; Biritwum, R.B.; Yawson, A.E.; Mensah, G.; Maximova, T.; et al. Chronic noncommunicable diseases in 6 low- and middle-income countries: Findings from wave 1 of the World Health Organization's study on global ageing and adult health (SAGE). *Am. J. Epidemiol.* **2017**, *185*, 414–428. [CrossRef]
15. Hopkins, K.L.; Hlongwane, K.E.; Otwombe, K.; Dietrich, J.; Cheyip, M.; Olivier, J.; Van Rooyen, H.; Doherty, T.; Gray, G.E. The substantial burden of non-communicable diseases and HIV-comorbidity amongst adults: Screening results from an integrated HIV testing services clinic for adults in Soweto, South Africa. *eClinicalMedicine* **2021**, *38*, 101015. [CrossRef]
16. Mazibuko-Makena, Z. The potential of Fourth Industrial Revolution technologies to transform healthcare: The question of access for the marginalised. In *Leap 4.0. African Perspectives on the Fourth Industrial Revolution*; Mazibuko-Makena, Z., Kraemer-Mbula, E., Eds.; Mapungubwe Institute for Strategic Reflection (MISTRA): Johannesburg, South Africa, 2021; pp. 287–316.
17. Liverani, M.; Ir, P.; Perel, P.; Khan, M.; Balabanova, D.; Wiseman, V. Assessing the potential of wearable health monitors for health system strengthening in low- and middle-income countries: A prospective study of technology adoption in Cambodia. *Health Policy Plan.* **2022**, *37*, 943–951. [CrossRef]
18. Noncommunicable Disease Alliance (NCD). *Optimising the Use of Digital Technologies for Healthy Societies and Economies*; Policy Brief; NCD Alliance: Geneva, Switzerland, 2023. Available online: https://ncdalliance.org/sites/default/files/resource_files/Digital_Health_Brief-2023-EN_0.pdf (accessed on 29 October 2025).
19. Jafleh, E.A.; Alnaqbi, F.A.; Almaeeni, H.A.; Faqeeh, S.; Alzaabi, M.A.; Al Zaman, K. The role of wearable devices in chronic disease monitoring and patient care: A comprehensive review. *Cureus* **2024**, *16*, e68921. [CrossRef]
20. Milani, R.V.; Bober, R.M.; Lavie, C.J. The role of technology in chronic disease care. *Prog. Cardiovasc. Dis.* **2016**, *58*, 579–583. [CrossRef]
21. Izu, L.; Scholtz, B.; Fashoro, I. Wearables and their potential to transform health management: A step towards sustainable development goal 3. *Sustainability* **2024**, *16*, 1850. [CrossRef]
22. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A.; Khalil, I.; Guizani, M.; Al-Fuqaha, A. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2456–2501. [CrossRef]
23. Ometov, A.; Shubina, V.; Klus, L.; Skibińska, J.; Saafi, S.; Pascacio, P.; Flueratoru, L.; Quezada-Gaibor, D.P.; Chukhno, N.; Chukhno, O.; et al. A survey on wearable technology: History, state-of-the-art and current challenges. *Comput. Netw.* **2021**, *193*, 108074. [CrossRef]
24. de Arriba-Pérez, F.; Caeiro-Rodríguez, M.; Santos-Gago, J.M. Collection and processing of data from wrist wearable devices in heterogeneous and multiple-user scenarios. *Sensors* **2016**, *16*, 1538. [CrossRef]
25. Bada, M.; von Solms, B. A cybersecurity guide for using fitness devices. In *The Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021*; Springer International Publishing: Cham, Switzerland, 2022; pp. 35–45.
26. Ching, K.W.; Singh, M.M. Wearable technology devices security and privacy vulnerability analysis. *Int. J. Netw. Secur. Its Appl.* **2016**, *8*, 19–30. [CrossRef]
27. Clausing, E.; Schiefer, M.; Lösche, U.; Morgenstern, M. *Internet of Things: Security Evaluation of Nine Fitness Trackers; Version 1.02*; Technical Report; AV-TEST GmbH: Magdeburg, Germany, 2015. Available online: https://www.av-test.org/fileadmin/pdf/avtest_2015-06_fitness_tracker_english.pdf (accessed on 12 February 2026).
28. Rahman, M.; Carbunar, B.; Banik, M. Fit and vulnerable: Attacks and defenses for a health monitoring device. In Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P), San Francisco, CA, USA, 19–22 May 2013. Available online: https://arxiv.org/pdf/1304.5672 (accessed on 1 September 2026).

29. Zendehdel, G.A. A Semi-Automated Security Assessment Framework for Wearable Health Monitoring Devices. Master's Thesis, University of New Brunswick, Fredericton, NB, Canada, 2020.
30. Lee, L.; Egelman, S.; Lee, J.H.; Wagner, D. Risk perceptions for wearable devices. *arXiv* **2015**, arXiv:1504.05694. [CrossRef]
31. Winter, J.S.; Davidson, E. Investigating values in personal health data governance models. In Proceedings of the 23rd Americas Conference on Information Systems: A Tradition of Innovation, Boston, MA, USA, 10–12 August 2017; pp. 1577–1586.
32. Aliverti, A. Wearable technology: Role in respiratory health and disease. *Breathe* **2017**, *13*, e27–e36. [CrossRef]
33. Azodo, I.; Williams, R.; Sheikh, A.; Cresswell, K. Opportunities and challenges surrounding the use of data from wearable sensor devices in health care: Qualitative interview study. *J. Med. Internet Res.* **2020**, *22*, e19542. [CrossRef]
34. Kariotis, T.; Ball, M.P.; Tzovaras, B.G.; Dennis, S.; Sahama, T.; Johnston, C.; Almond, H.; Borda, A. Emerging health data platforms: From individual control to collective data governance. *Data Policy* **2020**, *2*, e13. [CrossRef]
35. Bouderhem, R. Privacy and regulatory issues in wearable health technology. *Eng. Proc.* **2023**, *58*, 87. [CrossRef]
36. Kitain, J. Beware of wearables: Protecting privacy in a data-collecting world. *Drexel Law Rev.* **2016**, *9*, 1–30.
37. Data Management Association International. *DAMA-DMBOK: Data Management Body of Knowledge*, 2nd ed.; Technics Publications: Sedona, AZ, USA, 2017.
38. Khatri, V.; Brown, C.V. Designing data governance. *Commun. ACM* **2010**, *53*, 148–152. [CrossRef]
39. Katurura, M.; Cilliers, L. Privacy in wearable health devices: How does POPIA measure up? In *Proceedings of the 4th International Conference on the Internet, Cyber Security and Information Systems (ICICIS)*; Njenga, K., Ed.; Kalpa Publications in Computing; EasyChair: Manchester, UK, 2019; Volume 12, pp. 112–122.
40. Taka, A.M. A deep dive into dynamic data flows, wearable devices, and the concept of health data. *Int. Data Priv. Law* **2023**, *13*, 124–140. [CrossRef]
41. Tziouras, J. Health Data from Wearable Technologies: Privacy and Security Regulatory Aspects. Master's Thesis, Tilburg University, Tilburg, The Netherlands, 2022.
42. Winter, J.S.; Davidson, E. Harmonising regulatory regimes for the governance of patient-generated health data. *Telecommun. Policy* **2022**, *46*, 102285. [CrossRef]
43. Mattison, G.; Canfell, O.; Forrester, D.; Dobbins, C.; Smith, D.; Töyräs, J.; Sullivan, C. The influence of wearables on health care outcomes in chronic disease: Systematic review. *J. Med. Internet Res.* **2022**, *24*, e36690. [CrossRef]
44. EBSCO. Perception. EBSCO Research Starters. 2024. Available online: https://www.ebsco.com/research-starters/psychology/perception (accessed on 2 March 2026).
45. Ayers, T. Self-Regulation Within the Wearable Device Industry and the Alignment to Device Users' Perceptions of Health Data Privacy. Master's Thesis, Rochester Institute of Technology, Rochester, NY, USA, 2018.
46. Thomason, J. Big tech, big data and the new world of digital health. *Glob. Health J.* **2021**, *5*, 165–168. [CrossRef]
47. Chong, K.P.; Woo, B.K. Emerging wearable technology applications in gastroenterology: A review of the literature. *World J. Gastroenterol.* **2021**, *27*, 1149–1160. [CrossRef]
48. Dian, F.J.; Vahidnia, R.; Rahmati, A. Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A survey. *IEEE Access* **2020**, *8*, 69200–69211. [CrossRef]
49. Li, C.; Lin, S.H.; Chib, A. The state of wearable health technologies: A transdisciplinary literature review. *Mob. Media Commun.* **2021**, *9*, 353–376. [CrossRef]
50. Peng, C.; Xi, N.; Zhao, H.; Hamari, J. Acceptance of wearable technology: A meta-analysis. In Proceedings of the 55th Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2022; pp. 5101–5110.
51. Alzghaibi, H. Adoption barriers and facilitators of wearable health devices with AI integration: A patient-centred perspective. *Front. Med.* **2025**, *12*, 1557054. [CrossRef]
52. Cheung, M.L.; Chau, K.Y.; Lam, M.H.S.; Tse, G.; Ho, K.Y.; Flint, S.W.; Broom, D.R.; Tso, E.K.H. Examining consumers' adoption of wearable healthcare technology: The role of health attributes. *Int. J. Environ. Res. Public Health* **2019**, *16*, 2257. [CrossRef]
53. Smuck, M.; Odonkor, C.A.; Wilt, J.K.; Schmidt, N.; Swiernik, M.A. The emerging clinical role of wearables: Factors for successful implementation in healthcare. *npj Digit. Med.* **2021**, *4*, 45. [CrossRef]
54. Asif, M.; Gaur, P. The impact of digital health technologies on chronic disease management. *Telehealth Med. Today* **2025**, *10*, 556. [CrossRef]
55. Becker, M.; Matt, C.; Widjaja, T.; Hess, T. Understanding privacy risk perceptions of consumer health wearables—An empirical taxonomy. In Proceedings of the 38th International Conference on Information Systems (ICIS 2017), Seoul, Republic of Korea, 10–13 December 2017.
56. Datta, P.; Namin, A.S.; Chatterjee, M. A survey of privacy concerns in wearable devices. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 4549–4553.
57. Quévat, A.; Heinze, A. The digital transformation of preventive telemedicine in France based on the use of connected wearable devices. *Glob. Bus. Organ. Excell.* **2020**, *39*, 17–27. [CrossRef]

58. Arkenberg, C. Why Consumers and Doctors Are Wary About Wearable Data: Consumer Wearable Companies Are Smart to Watch for Compliance and Privacy Concerns. Deloitte Insights 2021. Available online: https://www.deloitte.com/us/en/insights/industry/technology/wearable-technology-healthcare-data.html (accessed on 24 June 2022).
59. Hänsel, K.; Wilde, N.; Haddadi, H.; Alomainy, A. Challenges with current wearable technology in monitoring health data and providing positive behavioural support. In *MOBIHEALTH'15: Proceedings of the 5th EAI International Conference on Wireless Mobile Communication and Healthcare, London, Great Britain, 14–16 October 2015*; Alomainy, A., Whittow, W., Hao, Y., Nechayev, K.S., Parini, C.G., Eds.; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2015; pp. 158–161.
60. Muzny, M.; Henriksen, A.; Giordanengo, A.; Muzik, J.; Grøttland, A.; Blixgård, H.; Hartvigsen, G.; Årsand, E. Dataset of wearable sensors with possibilities for data exchange. *Data Brief* **2020**, *28*, 104978. [CrossRef]
61. Lu, L.; Zhang, J.; Xie, Y.; Gao, F.; Xu, S.; Wu, X.; Ye, Z. Wearable health devices in health care: Narrative systematic review. *JMIR mHealth uHealth* **2020**, *8*, e18907. [CrossRef]
62. Huhn, S.; Axt, M.; Gunga, H.C.; Maggioni, M.A.; Munga, S.; Obor, D.; Sié, A.; Boudo, V.; Bunker, A.; Sauerborn, R.; et al. The impact of wearable technologies in health research: Scoping review. *JMIR mHealth uHealth* **2022**, *10*, e34384. [CrossRef]
63. Guk, K.; Han, G.; Lim, J.; Jeong, K.; Kang, T.; Lim, E.K.; Jung, J. Evolution of wearable devices with real-time disease monitoring for personalized healthcare. *Nanomaterials* **2019**, *9*, 813. [CrossRef]
64. Vijayan, V.; Connolly, J.P.; Condell, J.; McKelvey, N.; Gardiner, P. Review of wearable devices and data collection considerations for connected health. *Sensors* **2021**, *21*, 5589. [CrossRef]
65. Nahavandi, D.; Alizadehsani, R.; Khosravi, A.; Acharya, U.R. Application of artificial intelligence in wearable devices: Opportunities and challenges. *Comput. Methods Programs Biomed.* **2022**, *213*, 106541. [CrossRef]
66. de Arriba Pérez, F.; Santos-Gago, J.M.; Caeiro-Rodríguez, M.; Iglesias, M.J.F. Evaluation of commercial-off-the-shelf wrist wearables to estimate stress on students. *J. Vis. Exp.* **2018**, *136*, e57590. [CrossRef]
67. Mbekwa, N.; Adebesin, F. Not missing a step: South Africans taking control of their personal wellbeing using wearable health devices. *J. Health Inform. Afr.* **2019**, *6*, 11–18. [CrossRef]
68. Abdelhamid, M. Fitness tracker information and privacy management: Empirical study. *J. Med. Internet Res.* **2021**, *23*, e23059. [CrossRef]
69. Jain, P.; Gyanchandani, M.; Khare, N. Big data privacy: A technological perspective and review. *J. Big Data* **2016**, *3*, 25. [CrossRef]
70. Doherty, C.; Baldwin, M.; Keogh, A.; Caulfield, B.; Argent, R. Keeping pace with wearables: A living umbrella review of systematic reviews evaluating the accuracy of consumer wearable technologies in health measurement. *Sports Med.* **2024**, *54*, 2907–2926. [CrossRef]
71. Izu, L.; Scholtz, B.; Fashoro, I. A conceptual model of the benefits and concerns of wearable health data management. In *Smart and Secure Embedded and Mobile Systems—ICTA-EMOS 2022*; Springer Nature: Cham, Switzerland, 2024; pp. 193–203.
72. Ladley, J. *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program*; Academic Press: Cambridge, MA, USA, 2020.
73. Winter, J.S.; Davidson, E. Big data governance of personal health information and challenges to contextual integrity. *Inf. Soc.* **2019**, *35*, 36–51. [CrossRef]
74. Winter, J.S.; Davidson, E. Governance of artificial intelligence and personal health information. *Digit. Policy Regul. Gov.* **2019**, *21*, 280–290. [CrossRef]
75. Data Governance Institute. Definitions of Data Governance. Available online: https://datagovernance.com/the-data-governance-basics/ (accessed on 20 August 2023).
76. Rosenbaum, S. Data governance and stewardship: Designing data stewardship entities and advancing data access. *Health Serv. Res.* **2010**, *45*, 1442–1455. [CrossRef]
77. Kerr, D.; Butler-Henderson, K.; Sahama, T. Security, privacy, and ownership issues with the use of wearable health technologies. In *Managing Security Issues and the Hidden Dangers of Wearable Technologies*; Marrington, A., Kerr, D., Gammack, J., Eds.; IGI Global: Hershey, PA, USA, 2019; pp. 161–181. [CrossRef]
78. Lewy, H. Wearable technologies—Future challenges for implementation in healthcare services. *Healthc. Technol. Lett.* **2015**, *2*, 2–5. [CrossRef]
79. Sankin, A. Your Medical Data Is for Sale, and There's Nothing You Can Do About It. Reveal, 2017. Available online: https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/ (accessed on 21 July 2023).
80. Murdoch, T.B.; Detsky, A.S. The inevitable application of big data to health care. *JAMA* **2013**, *309*, 1351–1352. [CrossRef]
81. Creswell, J.W.; Creswell, J.D. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, 6th ed.; SAGE: Thousand Oaks, CA, USA, 2023.
82. Murairwa, S. Voluntary sampling design. *Int. J. Adv. Res. Manag. Soc. Sci.* **2015**, *4*, 185–200.
83. Saunders, M.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*, 8th ed.; Pearson: Harlow, UK, 2019.
84. Leedy, P.D.; Ormrod, J.E.; Johnson, L.R. *Practical Research: Planning and Design*, 12th ed.; Pearson Education: Harlow, UK, 2021.

85. Walliman, N. *Social Research Methods*; Routledge: Abingdon, UK, 2011.
86. Cohen, L.; Manion, L.; Morrison, K. *Research Methods in Education*, 8th ed.; Routledge: Abingdon, UK, 2018.
87. Gravetter, F.J.; Wallnau, L.B. *Statistics for the Behavioral Sciences*, 10th ed.; Cengage Learning: Boston, MA, USA, 2016.
88. Saunders, M.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*, 9th ed.; Pearson: Harlow, UK, 2023.
89. Braun, V.; Clarke, V. Thematic analysis. In *APA Handbook of Research Methods in Psychology*; Cooper, H., Camic, P.M., Long, D.L., Panter, A.T., Rindskopf, D., Sher, K.J., Eds.; American Psychological Association: Washington, DC, USA, 2012; Volume 2, pp. 57–71. [CrossRef]
90. Braun, V.; Clarke, V. *Thematic Analysis: A Practical Guide*; SAGE Publications: London, UK, 2022.
91. Cilliers, L. Wearable devices in healthcare: Privacy and information security issues. *Health Inf. Manag. J.* **2020**, *49*, 150–156. [CrossRef]
92. Hoffman, A.; Masucci, R. *Protecting Individuals' Privacy and Data in the Artificial Intelligence World*; Intel's AI Privacy Policy White Paper; Intel Corporation: Santa Clara, CA, USA, 2018; pp. 1–9. Available online: https://community.intel.com/legacyfs/online/files/Intels-AI-Privacy-Policy-White-Paper-2018.pdf (accessed on 13 March 2024).
93. Mehmood, A.; Natgunanathan, I.; Xiang, Y.; Hua, G.; Guo, S. Protection of big data privacy. *IEEE Access* **2016**, *4*, 1821–1834. [CrossRef]
94. Lowens, B.; Motti, V.G.; Caine, K. Wearable privacy: Skeletons in the data closet. In *Proceedings of the 2017 IEEE International Conference on Healthcare Informatics, Park City, UT, USA, 23–26 August 2017*; Cummins, M., Facelli, J., Meixner, G., Giraud-Carrier, C., Nakajima, H., Eds.; IEEE: Piscataway, NJ, USA, 2017; pp. 295–304. [CrossRef]
95. Els, F.; Cilliers, L. Improving the information security of personal electronic health records to protect a patient's health information. In *Proceedings of the 2017 Conference on Information Communication Technology and Society (ICTAS), Durban, South Africa, 6–7 March 2017*; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
96. Kuznetsov, M.; Novikova, E.; Kotenko, I.; Doynikova, E. Privacy policies of IoT devices: Collection and analysis. *Sensors* **2022**, *22*, 1838. [CrossRef]
97. Lee, J.; Kim, D.; Ryoo, H.Y.; Shin, B.S. Sustainable wearables: Wearable technology for enhancing the quality of human life. *Sustainability* **2016**, *8*, 466. [CrossRef]
98. Horvitz, E.; Mulligan, D. Data, privacy, and the greater good. *Science* **2015**, *349*, 253–255. [CrossRef]
99. Mone, V.; Shakhlo, F. Health data on the go: Navigating privacy concerns with wearable technologies. *Leg. Inf. Manag.* **2023**, *23*, 179–188. [CrossRef]
100. Zuboff, S. Surveillance capitalism and the challenge of collective action. *New Labor Forum* **2019**, *28*, 10–29. [CrossRef]
101. Sekalala, S.; Rawson, B.; Andanda, P. A socio-legal critique of the commercialization of digital health in Sub-Saharan Africa. *Policy Stud.* **2025**, *47*, 285–305. [CrossRef]
102. Minbaleev, A.V.; Nikolskaia, K.Y.; Zhernova, V.M. Legal enforcement of cybersecurity of wearable mobile devices in healthcare. In *Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy*; Nazarov, A., Ed.; Atlantis Press: Amsterdam, The Netherlands, 2020; Volume 156, pp. 674–678. [CrossRef]
103. Piwek, L.; Ellis, D.A.; Andrews, S.; Joinson, A. The rise of consumer health wearables: Promises and barriers. *PLoS Med.* **2016**, *13*, e1001953. [CrossRef]
104. Bradshaw, A. Building a Data Governance Strategy in 7 Steps. Alation, 15 December 2021. Available online: https://www.alation.com/blog/steps-for-building-data-governance-strategy/#:~:text=A%20data%20governance%20strategy%20provides,will%20collect%20and%20manage%20data (accessed on 24 July 2023).
105. Mahanti, R. *Data Governance Success: Growing and Sustaining Data Governance*; Springer Nature Singapore Pte Ltd.: Singapore, 2021.
106. Obatolu, R. A Holistic Framework for Complex Big Data Governance. Ph.D. Thesis, University of East London, London, UK, 2022.
107. Patel, U. Information technology strategy: A case for data governance. *Procedia Comput. Sci.* **2022**, 2314–2516. Available online: https://easychair.org/publications/preprint/mFbx/download (accessed on 9 June 2024).

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