Received 24 December 2024
Revised 20 May 2025
15 September 2025
30 October 2025
8 December 2025
Accepted 25 January 2026

Mitigating resistance in smart health monitoring systems: the role of data governance and privacy concerns

Jingjing Zhang
Department of Management, Technology, and Organisation, Auckland University of Technology, Auckland, New Zealand
Farkhondeh Hassandoust
Department of Information Systems and Operation Management, The University of Auckland, Auckland, New Zealand, and
Allen C. Johnston
Department of Information Systems, Statistics, and Management Science, Culverhouse College of Business, The University of Alabama, Tuscaloosa, Alabama, USA

Abstract

Purpose – Smart health monitoring systems (SHMSs) have encountered resistance and limited adoption by various stakeholders. This study aims to investigate the impact of data governance on the associated privacy concerns in relation to barriers, thereby mitigating users' resistance to SHMSs.

Design/methodology/approach – This mixed-methods study draws on innovation resistance theory and data governance mechanisms. We developed a research model based on 20 qualitative interviews with individuals from multiple stakeholder groups and empirically tested the model using 277 valid responses from potential and current SHMS users, collected through an online questionnaire survey.

Findings – The findings reveal that data governance mechanisms–incorporating legislative protection, cultural and religious differences (procedural data governance mechanisms), transparency, and trust (relational data governance mechanisms)–are more influential than accountability and responsibility (structural data governance mechanisms) in reducing user resistance to SHMSs. Privacy concerns significantly influence functional barriers to SHMSs and ultimately positively affect users' resistance to SHMSs. Cultural and religious differences and trust mechanisms are significantly associated with privacy concerns among users with a high personal innovativeness level.

Research limitations/implications – The study extends innovation resistance theory by integrating data governance, showing how theoretical models can be practically adapted for diverse health information technology (HIT) contexts. The findings offer societal implications, informing policies that promote SHMS development with robust privacy protections, inclusive design and trust-building governance.

Originality/value – This is a pioneering study that extends innovation resistance theory by integrating data governance, demonstrating how theoretical models can be tailored to address diverse needs within the HIT domain.

Keywords Innovation resistance theory, Data governance, Privacy concerns, Functional barriers, Smart health monitoring

Paper type Research article

1. Introduction

Smart health monitoring systems (SHMSs) have emerged as a prevalent form of digital surveillance technology, utilizing real-time monitoring and sensor-based health applications to track users' vital signs and daily health conditions (Almujally *et al.*, 2023). These systems

Internet Research
Vol. 36 No. 7, 2026
pp. 82-106
Emerald Publishing Limited
e-ISSN: 2054-5657
p-ISSN: 1066-2243
DOI 10.1108/INTR-12-2024-2032

include devices such as blood glucose wearables and electrocardiogram (ECG) monitors, which are crucial for the functionality of SHMSs (Stavropoulos *et al.*, 2020). The rapid growth of SHMSs in recent years can be attributed to innovations in digital surveillance technologies (Clarke, 2019) that have shown a variety of anticipated benefits, including improved communication between patients and healthcare providers, lower costs for professional visits, and more effective diagnostic and treatment processes, among others (Salehi-Amiri *et al.*, 2022). The global SHMS market, valued at USD $190 billion in 2024, is projected to grow to USD $474 billion by 2032 (GlobeNewswire, 2023; Market.Us, 2023).

Despite significant investments based on their anticipated benefits, SHMSs have faced resistance and limited diffusion from multiple stakeholders. A global mHealth review found that over half of end-users reported issues that prompted them to uninstall the services, with many leaving 1-star ratings (Haggag *et al.*, 2022). These challenges stem from various barriers, including resistance to change, concerns about trustworthiness, fatigue and technostress, lack of ability to operate smart devices, and transition costs (Iyanna *et al.*, 2022; Talwar *et al.*, 2023).

Among the cited barriers to SHMS adoption, the psychological barrier of privacy concerns stands out (Pal *et al.*, 2019; Smith *et al.*, 2011). Multiple global reports (e.g. Accenture.com, 2020; Capterra.com, 2021; Fortune.com, 2023) highlight privacy concerns as the primary factor driving consumers' resistance to the adoption of SHMSs and reluctance to share health data with healthcare professionals. These concerns are primarily linked to the surveillance technologies embedded in SHMS systems. In particular, such technologies often create confusion or uncertainty regarding responsibility in the event of personal health data loss and the assurance of protecting and properly using these data within the surveillance framework. Ambiguities in data regulation policies further complicate this issue, as they often fail to clearly define accountability (Duckert and Barkhuus, 2022; Princi and Krämer, 2020). These uncertainties are deeply connected to data governance, which is responsible for assigning authority and control over data, as well as overseeing the authority through decision-making in data-related matters (DAMA International, 2009; Janssen *et al.*, 2020; Plotkin, 2020).

Alongside privacy concerns, other potential barriers causing resistance to innovative technologies have been explored, such as the complicated environments of SHMSs, security issues, complexity of innovation, and lack of perceived value (Chouk and Mani, 2019; Prakash and Das, 2022). Privacy concerns can amplify or lead to functional barriers across various health information technology (HIT) contexts. For example, privacy concerns have been shown to limit the perceived value of Internet of Things (IoT)-based smart home services (Kim *et al.*, 2017). In a transformed health ecosystem, the complexity and dynamic nature of the system can further intensify privacy and security challenges (Ruotsalainen and Blobel, 2022). Although both psychological and functional barriers contribute equally to resistance to SHMSs, privacy concerns have been found to positively correlate with functional barriers, such as perceived technical complexity and the value of smart health products (Dhagarra *et al.*, 2020; Kim *et al.*, 2017; Mani and Chouk, 2017). Moreover, effective data governance plays a critical role in managing privacy concerns, mitigating risks, and balancing competing interests within the complex landscape of health data sharing across multidisciplinary contexts (Knoppers and Thorogood, 2017).

To dissect these barriers to SHMSs, it is essential to understand their origins and impacts in order to mitigate them through effective data governance and relevant means (Hunter *et al.*, 2020). However, a review of recent research reveals a notable gap: few studies have explicitly examined how data governance can alleviate privacy concerns and other barriers resulting in users' resistance to SHMSs (Chibuike *et al.*, 2024; Davidson *et al.*, 2023; Yaqoob *et al.*, 2022). The review analysis is presented in Table S1 of the supplementary document, accompanied by a brief explanation.

Against this backdrop, we explore the role of data governance in relation to the concerns and barriers causing resistance to SHMS adoption, drawing on innovation resistance theory (Ram and Sheth, 1989) and data governance mechanisms (Abraham *et al.*, 2019). The research questions (RQs) that drive this study are: (RQ1) *What are the contributing elements of data*

governance mechanisms in relation to users' resistance to SHMSs? And (RQ2) *How and in what ways do data governance mechanisms influence individuals' concerns and barriers in terms of mitigating SHMS resistance*? This study extends innovation resistance theory through the integration of data governance mechanisms, a novel approach that responds to the growing complexity of user concerns about SHMSs.

By doing so, it not only broadens the scope of the theory but also refines our understanding of how psychological and functional barriers co-evolve through the lens of privacy concerns. In particular, we show that relational governance mechanisms (e.g. transparency and trust) are theoretically positioned to influence sustained engagement and reduce resistance, particularly by building user confidence and relational trust, a nuance not fully explored in existing models. While our study is cross-sectional, the findings highlight associations that align with this proposed mechanism. This integration offers a theoretical bridge between technology resistance literature and data governance research, highlighting governance as an active, moderating influence, rather than a passive concept. Practically, these insights guide both policymakers and service designers in addressing privacy, complexity, and value-related resistance in SHMS environments.

2. Literature review

2.1 Concerns and barriers related to SHMSs

In highly innovative contexts such as SHMSs, the phenomenon of technology adoption resistance often arises from the interplay of privacy concerns, usage barriers, perceived complexity, and the recognition of value. Privacy has emerged as a persistent social concern linked to the development of innovative information technologies that enable pervasive surveillance, the creation of large-scale databases, and the rapid global distribution of information (Nissenbaum, 2010; Timan and Albrechtslund, 2018). However, recent developments such as the integration of blockchain and federated learning have been proposed to enhance privacy preservation in digital health systems, offering secure, decentralized, and collaborative models of patient data sharing that balance data utility with confidentiality (Alsamhi *et al.*, 2024). Privacy concerns, as psychological barriers against undesirable intrusion during surveillance activities (Harris, 2020; Solove, 2006), are people's perceptions of what happens with the data they provide or share with others (Bélanger and Crossler, 2011; Crossler and Bélanger, 2019). Due to their ability to capture detailed contextual information about individuals, the use of surveillance or monitoring applications without appropriate privacy protection mechanisms increases privacy concerns and, therefore, leads to resistance against smart health applications (Pirzada *et al.*, 2021; Prati *et al.*, 2019).

Previous studies have also reported various functional barriers that result in the failure and rejection of new technologies. Complexity barriers (e.g. contact tracing or mobile payment) can challenge users with low technical skills or limited experience, as compared to conventional methods (Kaur *et al.*, 2020; Prakash and Das, 2022), while value barriers arise when users perceive the costs of adoption to outweigh the benefits (Iyanna *et al.*, 2022; Mani and Chouk, 2017). Research has investigated the direct effects of both psychological and functional barriers on resistance to smart technology innovations (Chouk and Mani, 2019; Hew *et al.*, 2019; Prakash and Das, 2022). Notably, privacy concerns have also been found to correlate with functional barriers that can ultimately influence users' resistance (e.g. Dhagarra *et al.*, 2020; Kim *et al.*, 2017; Mani and Chouk, 2017). For example, privacy issues have been associated with perceived sacrifice, which in turn affects the perceived value of smart home products (Kim *et al.*, 2017).

2.2 Data governance for SHMSs

Prior research suggests that data governance mechanisms can help mitigate user resistance to technology adoption (Abraham *et al.*, 2019). Data governance mechanisms refer to control

mechanisms and procedures used to manage health data and support responsible data sharing —allowing access when necessary, restricting it when not, and ensuring the privacy and confidentiality of all stakeholders (DAMA International, 2009; Janssen *et al.*, 2020). These mechanisms are widely recognized as effective tools for addressing user privacy concerns, particularly in technology-driven, data-intensive environments, with demonstrated impact across healthcare (Abraham *et al.*, 2019), e-commerce (Trampusch, 2024), Fintech-embedded banking (Wang *et al.*, 2023), and AI-driven contexts (Lewis and Moorkens, 2020).

Data governance mechanisms can be categorized into s*tructural*, *procedural*, and *relational* mechanisms. *Structural* mechanisms focus on identifying key decision-makers and their roles and responsibilities regarding data ownership, cost management, and value assessment (Abraham *et al.*, 2019; Tallon, 2013). These mechanisms are characterized by formalized roles, rules, and clear reporting structures (Abraham *et al.*, 2019). Central themes include accountability and responsibility, which are closely tied to institutional obligations and decision authority (Abraham *et al.*, 2019). *Procedural* mechanisms encompass the operational rules and safeguards that govern how data is managed, accessed, and shared. These mechanisms are designed to ensure that data is shared appropriately and lawfully, recorded reliably and accurately, used ethically and effectively, and held securely and confidentially (Borgman *et al.*, 2016; Schneider *et al.*, 2023). In particular, procedural mechanisms aim to support data-related issue management across legislative, cultural, religious, and technical innovation processes (DAMA International, 2009). *Relational* governance mechanisms facilitate collaboration among stakeholders by focusing on key areas such as communication, training, and coordinated decision-making (Abraham *et al.*, 2019). These mechanisms are instrumental in building trust, with transparency often serving as a critical component of relational trust-building (Elahi *et al.*, 2019; Mabillard *et al.*, 2021). Accordingly, this study considers trust and transparency as central elements of relational governance mechanisms, while remaining open to other emergent themes identified through interview findings.

Given the importance of exploring salient elements across multiple levels to address the privacy issues that lead to customers' resistance to SHMSs, numerous scholars have investigated multi-level antecedents to this resistance (e.g. Iyanna *et al.*, 2022; ParkKim *et al.*, 2022; Xu, 2019). However, there is insufficient information on how these contributing elements can be mitigated through regulatory mechanisms, underscoring the need for data governance-based solutions (Chibuike *et al.*, 2024; Davidson *et al.*, 2023).

2.3 Innovation resistance theory

Innovation resistance theory, developed by Ram and Sheth (1989), explains the reasons behind customers' resistance to adopting innovations despite their perceived desirability and necessity. It assumes that individuals resist adopting modern technologies either because these technologies require customers to potentially change from a satisfactory existing state or because they contradict customers' belief structure (ParkWerder *et al.*, 2022; Ram and Sheth, 1989). According to the theory, the main reasons for innovation resistance can be categorized as psychological and functional barriers (Ram and Sheth, 1989). These barriers, such as perceived privacy concerns, complexity, value, usage, and risk, have consistently been identified as key antecedents of resistance to SHMS, regardless of their interrelationships (e.g. Chouk and Mani, 2019; Kim *et al.*, 2017; Prakash and Das, 2022).

This study draws on innovation resistance theory to understand barriers that influence SHMS resistance. We focus on privacy concerns as a key psychological barrier, and include three widely recognized functional barriers: usage, complexity, and value barriers (Chouk and Mani, 2019; Kim *et al.*, 2017). These barriers have been consistently cited in digital health resistance literature as primary determinants of user hesitation. Other barriers such as risk, tradition, and image are not included due to their limited empirical relevance in the SHMS context or their conceptual overlap with the selected constructs.

3. Mixed-method research design and results

This study followed a post-positivist research paradigm (Creswell and Poth, 2018), using a sequential two-stage mixed-methods design comprising both qualitative and quantitative analyses (Creswell and Plano Clark, 2018). This specific methodology was selected because of its key methodological advantages, including its ability to facilitate a comprehensive understanding and synthesis of insights derived from qualitative and quantitative dimensions, thereby balancing depth and breadth (Venkatesh *et al.*, 2013). Our mixed-methods approach was structured around a developmental purpose with two study phases (Study 1 and Study 2). Study 1 was a qualitative study, the findings of which were used to develop a suitable set of constructs, establish relationships among these constructs in the form of a model, and propose a corresponding set of hypotheses. In Study 2, these hypotheses were tested using a quantitative method (Venkatesh *et al.*, 2016).

3.1 Study 1: qualitative study design

Study 1 followed an explorative research approach with purposive sampling to recruit participants familiar with SHMSs (Creswell and Poth, 2018). The study involved 20 qualitative interviews with individuals from multiple stakeholder groups, including front-line healthcare providers, government health authorities, technology providers, and end-users with either direct user experience or a strong interest in smart devices. Participant demographics are provided in Table S2 (in the supplementary document), where 10 interviewees are identified as end-users. The interviews aimed to identify key contextual factors related to data governance mechanisms and innovation resistance theory to inform the development of the research model and hypotheses. Participants discussed various SHMS scenarios, ranging from clinical trial applications to commercially available monitoring devices such as glucose monitors.

Guided by Taylor *et al.* (2016), the semi-structured interviews averaged 45 min. Each session began with warm-up demographic questions, such as participants' familiarity with the described SHMS. The discussion then moved to research-focused questions derived from the literature and tailored to the smart health context, particularly data governance mechanisms (Abraham *et al.*, 2019). Participants were invited to reflect on factors influencing resistance to SHMSs, including structural governance elements. For example, they were asked, "What factors (or characters) should be included in the reporting structure to protect your data privacy and address concerns when they arise?"

Following previous studies (e.g. Coert *et al.*, 2021; Fox and Hoy, 2019; Matt *et al.*, 2019; Zuzul, 2019), data collection ceased after 20 interviews, as no new insights emerged, indicating theoretical saturation (Glaser and Strauss, 1967). All interviews were audio-recorded and fully transcribed. The first author coded the transcripts in NVivo v12, and the second author reviewed the coding and analysis. We then conducted a thematic analysis to identify key themes and patterns related to data governance mechanisms that mitigate users' concerns and resistance to SHMSs. Thematic analysis is a common method for analyzing and reporting patterns or themes in qualitative data (Braun and Clarke, 2006).

3.2 Developing and hypothesizing SHMS users' resistance model

From the reviewed literature and interview results, we identified seven key elements across three aspects of data governance mechanisms in relation to privacy concerns about SHMSs: *accountability* and *responsibility* (structural mechanisms); *legislative protection*, *cultural and religious differences*, and *traceability* (procedural mechanisms); *transparency* and *trust* (relational mechanisms). These elements addressed RQ1 and informed the development of the quantitative model to answer RQ2. Table S3 (see the supplementary document) presents selected quotes that illustrate key constructs and relationships.

Accountability and responsibility are considered two critical elements of structural data governance mechanisms, as they pertain to institutional obligations and decision-making authority (Abraham *et al.*, 2019). *Accountability* refers to stakeholders being asked to account

for their actions to an authority (van Donge *et al.*, 2022). In health information systems, accountability involves assigning legal responsibility to an organization that handles personal health data in SHMSs, ensuring that any contracted partners to whom it provides this data are compliant, regardless of their location (Pearson and Charlesworth, 2009). One participant (p#4) remarked, "*Accountability sounds important, but honestly, as a regular user, I don't really notice it or even know it's there. That makes it difficult for me to really care or support the system development*." She (p#4) added, "*For the same reason, it's hard to see how it [accountability] could meaningfully help address my privacy concerns*." Another participant (p#5) stated that, "*To keep health data safe and handle any related issues, it's really important to have clear [accountability]. In this way, everyone involved knows who's ultimately responsible if something goes wrong, which helps everyone feel more supported and secure*."

Responsibility is the overall relationship of the system with all its stakeholders, which involves being accountable for actions and fulfilling obligations or commitments (Dahlsrud, 2008; Ebrahim and Buheji, 2020). It has crucial implications for addressing data-related concerns, such as ethical dilemmas, fear, and dependence associated with emerging technologies in healthcare (Someh *et al.*, 2019). As an element of structural data governance mechanisms, most participants emphasized the importance of responsibilities and roles in an SHMS context from a management perspective. For example, a participant (p#11) stated that their company complied with relevant laws and regulations (such as the General Data Protection Regulation (GDPR)) by assigning a data protection officer to oversee and supervise data-related issues within their organizations. Another participant (p#2) stated, "*We have mechanisms for responsibility in charge of privacy violations in a digital innovation context*." He explained that if an individual user had a concern, they should be able to make a complaint and direct that concern to an officer who must use their authority to resolve the concern. He added, "*From the view of stakeholders' collaboration, responsibility-based mechanisms help increase the entire quality of the service and simplify complicated processes among various stakeholders*." Thus, we posit the following hypotheses:

H1. The structural data governance mechanisms of accountability are negatively associated with users' privacy concerns in relation to their resistance to SHMSs.

H2. The structural data governance mechanisms of responsibility are negatively associated with users' privacy concerns in relation to their resistance to SHMSs.

Procedural mechanisms address operational processes, compliance, and implementation standards (Schneider *et al.*, 2023; Tallon, 2013). In this study, *legislative protection*, *cultural and religious differences*, and *traceability* were categorized under procedural mechanisms. *Legislative protection* covers rights to information, restrictions on the use of data governance mechanisms, information technology (IT) security legislation, and support for the legal implementation of data governance (Weber, 2010). Legislative protection mechanisms play a crucial role in addressing privacy concerns, preserving personal autonomy, and mitigating skepticism toward technical innovations (Gasser *et al.*, 2020; Nguyen *et al.*, 2022; Princi and Krämer, 2020). All interviewees emphasized the importance of legislative protection in SHMS data management. Many were confident in their familiarity with local Privacy Acts and related codes or in their capability to access the acts for more legal information to address the potential issues about personal data and SHMS technologies. A participant (p#5) expressed, "*Effective legislative protection mechanisms can influence how users look at the value of the smart service . . . it is because robust health data protection mechanisms are critical for the overall value derived from data . . . and it is very helpful to simplify the process of our data protection activities when complying with the GDPR framework*." Thus, we posit the following hypothesis:

H3. The procedural data governance mechanism of legislative protection is negatively associated with users' privacy concerns in relation to their resistance to SHMSs.

While cultural and religious sensitivity may feel relational, its implementation tends to be procedural which is focused on compliance, standardization, and embedded workflows (Abraham *et al.*, 2019). A typical case would be the issue management when giving care to dying patients and defining the death process as a very tiring event with a scary end (Karadag *et al.*, 2019). Characterized as procedural safeguards for managing cultural and religious issues (DAMA International, 2009), cultural and religious differences play a pivotal role in shaping innovativeness, risk tolerance, and receptiveness to change. Such differences serve as critical elements in the design and effectiveness of procedural governance mechanisms (Schneider *et al.*, 2023). These elements shape interpretations of privacy-related issues and influence people's attitudes and behaviors when they use healthcare monitoring devices (Karadag *et al.*, 2019; Smith *et al.*, 2011). Nearly all interviewees highlighted the significance of cultural and religious differences in relation to associated concerns with SHMSs. One participant (p#9) stated, "*Cultural differences and religious diversity really need to be considered throughout the whole implementation process. It's about making sure people understand that their data is being collected, being held, and being accessed, and making sure that they're happy with all that fits. These things need to be carefully monitored, not just written down on paper.*" Thus, we posit the following hypothesis:

H4. The procedural data governance mechanisms of cultural and religious differences are positively associated with users' privacy concerns in relation to their resistance to SHMSs.

Traceability aids in identifying interconnectedness and enhancing analysis between SHMS devices and their data owners (Lomotey *et al.*, 2017). However, improper use of traceability has limitations in health data management. This can lead to consumer concerns and anxiety when consumers realize they are being traced, as various service providers can access their sensitive health data (Chouk and Mani, 2019; Ismail *et al.*, 2020). Our interview findings showed that *traceability* is a critical topic that potentially influences individuals' concerns about data protection practices among stakeholders. A participant (p#10) stressed, "*To be able to use that device within New Zealand, we have to switch off the voice recognition part, but there were questions such as can I be listened or can I be tracked?*" On the other hand, it is noteworthy to learn that traceability can contribute to the enhancement of health data protection practices and increase the service value of smart monitoring. One participant (p#4) pointed out, "*They [service providers] will be able to monitor improper data transfer processes. This [traceability] can avoid or detect unauthorized behaviors and increase the data protection ability of the system* [SHMS]*. . . In this sense, the tracing ability simplifies management and collaboration processes among service providers and reduces the feeling that the service is too complex to understand.*" Thus, we posit the following hypothesis:

H5. The procedural data governance mechanism of traceability is positively associated with users' privacy concerns in relation to their resistance to SHMSs.

Relational mechanisms are grounded in trust-building, transparency, and sustained engagement over time. Transparency and trust are central to this category (Borgman *et al.*, 2016; Xu, 2019). Interview findings highlighted *transparency* and *trust* as two critical elements of relational data governance mechanisms that could mitigate concerns related to the use of personal data in SHMSs. *Transparency* involves making everything visible, indicating openness or open communication to establish trustworthiness (Kim *et al.*, 2014). Transparency is closely associated with various issues surrounding users' resistance to SHMS usage, including mistrust, control, perceived privacy and security concerns, and cultural considerations (Talal *et al.*, 2019; Van Zoonen, 2016). Although prior research indicates that the impact of transparency varies according to individual privacy preferences (Bemmann *et al.*, 2022), one participant (p#2) nonetheless highlighted its importance, noting, "*You can always provide really clean and clear explanations, including a lot of detail, and that will give, like most people, won't care to go into that level of detail. But for the people*

that do, it's good to have that there and available for them." Moreover, one participant (p#5) mentioned, "*When we collect personal data from customers, we need to clearly explain our aim, behaviors . . . why we have to use it. By making the whole data sharing process open and transparent . . . customers can better understand the benefit or value from using it [device] and reduce reluctance to cooperate with us.*" Thus, we posit the following hypothesis:

H6. The relational data governance mechanism of transparency is negatively associated with users' privacy concerns in relation to their resistance to SHMSs.

Trusting beliefs have been identified as a predictor that influences the forming of psychological obstacles, such as fear of technological complexity and discomfort when being monitored by service providers (Elahi *et al.*, 2019; Puntoni *et al.*, 2021). Trust is important in data governance practices as it ensures the establishment of successful relationships and the management of risks and uncertainties (Abraham *et al.*, 2019; Chang and Fang, 2013). One interviewee (p#7) remarked, "*Overall, trust is an extremely important thing. It can even have a direct impact on the health index of the elderly.*" Another interviewee (p#4) stated, "*Trust can boost users' confidence in its potential value of the service and minimize perceived risks or difficulties, thereby encouraging users to give it a try.*" Thus, we posit the hypothesis:

H7. The relational data governance mechanism of trust is negatively associated with users' privacy concerns in relation to their resistance to SHMSs.

Privacy concerns related to personal data use are important psychological barriers that have contributed to users' resistance to new information technologies (e.g. Hew *et al.*, 2019; Zhu *et al.*, 2022). Further, privacy concerns may result in functional barriers that eventually impact consumers' acceptance of health monitoring devices (Sun *et al.*, 2024). In terms of the association between privacy concerns and usage barriers, perceived risk including privacy may affect functional barriers such as the perceived usefulness of smart home applications (Hubert *et al.*, 2019; Wang *et al.*, 2020). One participant (p#9) shared, "*In my experience, people often struggle with using a separate reading device rather than using their phone. They have to plug that into a computer and upload it, which can be especially challenging for older individuals to get the information onto the website. Ideally, they would come into the clinic, and the staff could assist them using a computer, but that requires a driver and IT access to . . .. I think very few people are willing to do this partly due to privacy concerns.*" Thus, we posit the following hypothesis:

H8. Privacy concerns are positively associated with usage barriers in relation to users' resistance to SHMSs.

Innovative technologies often require significant changes that conflict with existing usage patterns, creating complexity barriers. Similarly, privacy concerns can generate complexity barriers when individuals struggle to interact with SHMSs due to the complexities of data governance mechanisms for sharing and protection (Eagleson *et al.*, 2017; Friedman and Ormiston, 2022; Prakash and Das, 2022). As one participant (p#1) noted, "*People have privacy concerns based on assumptions that ask for better protection, better security, and better configurability. For example, when you access Facebook's settings, you'll find a variety of options—not because Facebook created them, but because users, driven by demand, pushed for them. I can see a similar trend unfolding in digital health contexts.*" Thus, we posit the following hypothesis:

H9. Privacy concerns are positively associated with complexity barriers in relation to users' resistance to SHMSs.

In terms of privacy concerns with value barriers, users' psychological states can help predict how they perceive the value of healthcare systems (Li *et al.*, 2023). One participant (p#2) emphasized the challenge between privacy and functional barriers, "*[Despite the purpose of*

reducing privacy concerns], potential users may find it complex to understand complicated legislative terms . . .. It's quite often to be asked to give more consents . . . it could deter them from recognizing the potential value of a smart device . . . or matching up with new rules." An interviewee (p#13) noted, "*I feel like the value of my smart device really drops when I start getting anxious about the privacy of my health information*." In addition, one participant (#9) shared, "*Privacy worries can make people hesitate to trust this service because, deep down, there's always that fear of personal information slipping out. When users feel their data isn't safe, it's hard for them to see the real value in using it.*" Thus, we posit the following hypothesis:

H10. Privacy concerns are positively associated with value barriers in relation to users' resistance to SHMSs.

Prior research shows that functional barriers positively affect resistance to innovative technologies (e.g. Mani and Chouk, 2017; Prakash and Das, 2022). For example, research indicates that a significant barrier to smart device usage is the concern that the device battery may quickly drain and require frequent recharging (Prakash and Das, 2022). Similarly, the interview results suggested that usage barriers are critical factors in customers' resistance to SHMSs. For instance, one participant (p#12) noted, "*Some patients found it challenging to remember to recharge or set up a smart device . . . which could deter them from wearing it.*" Thus, we posit the following hypothesis:

H11. Usage barriers are positively associated with users' resistance to SHMSs.

Perceived complexity refers to the degree to which consumers perceive a technology or application to be difficult to use (Anshu *et al.*, 2022). Recent literature on innovation resistance has identified complexity as a key factor contributing to users' reluctance to adopt smart services (Chibuike *et al.*, 2024; Mani and Chouk, 2017, 2018). Reflecting this notion, one participant (p#4) expressed, "*I find the appearance of the app looks a bit cluttered . . .. I think it should have a simpler design . . . it is complicated for me to manage my health data properly, for example, uploading the records in the correct location and removing them after a period for my privacy purpose.*" Thus, we posit the following hypothesis:

H12. Complexity barriers are positively associated with users' resistance to SHMSs.

Value barriers develop when consumers perceive innovation as incapable of delivering better functionalities than alternative options using the same economic resources (Hew *et al.*, 2019; Iyanna *et al.*, 2022). This understanding also matches interview comments in this study, where one participant (p#18) noted, "*I need to understand the value of new technology, whether it's actually beneficial for my health compared to the way I used to manage my treatment. If it doesn't appeal to me or offer something better, why should I use it?*" Thus, we posit the following hypothesis:

H13. Value barriers are positively associated with users' resistance to SHMSs.

In the context of SHMSs, self-efficacy reflects an individual's confidence in their capabilities to successfully perform a specific task, thus helping users overcome various functional barriers (Kumari and Kumar, 2023; ParkKim *et al.*, 2022). Technical self-efficacy may indirectly affect the relationship between the extent to which individuals view usage of digital health innovations as part of their identity and their adoption of these technologies (Maddah *et al.*, 2024; Reychav *et al.*, 2019). In line with the literature, one participant (p#3) shared her opinions about self-efficacy and usage barriers, noting that, "*My mother, who's still alive and is 89, lacks confidence in her ability to use new technology. She doesn't even want the Internet in her house because she finds it difficult to maintain and it's giving access to her information*." Another participant (p#18) shared, "*I've found that protecting my personal data privacy often means going through countless settings or giving disclaimers to others. These steps make me feel overwhelmed and powerless. Technically, I don't feel capable of handling it all, and it just*

makes me want to give up on using them." Technical self-efficacy may also moderate the impact of the perceived difficulty or complexity in adopting digital health services (Mensah *et al.*, 2022). Aligned with the extant literature, one participant (p#7) noted, "*I've heard that some of our customers have stopped using the monitoring device because the battery keeps running out. They found it frustrating, and they were just unable to manage the upkeep.*" Users with high self-efficacy are confident in their use of technology. They can resist using technologies that do not suit their needs and instead use those that do, or wait until other opportunities present themselves. However, such users are more likely to recognize the value of health monitoring applications (Okazaki *et al.*, 2013). Similarly, our findings also revealed the self-efficacy effects on the relationship between value barriers and users' resistance to SHMSs. One participant (p#19) highlighted, "*Many times, if I don't have strong skills in operating high-tech products, it does affect my judgment of their value. So I tend to think they can't really help me. At the same time, if I anticipate that the device offers little value to me, I definitely won't be willing to use it.*" Based on the above statements, hypotheses are proposed as follows:

H14(a-c). Self-efficacy moderates the effects of (a) usage barriers, (b) complexity barriers, and (c) value barriers on users' resistance to SHMSs.

Based on the extant literature and qualitative results, as well as the posited hypotheses, we propose a concern mitigation data governance model targeting SHMS users' resistance, as shown in Figure 1.

3.3 Study 2: quantitative study design

Following a mixed-methods design, Study 2 empirically tested the proposed model (Figure 1) among individuals familiar with an SHMS or currently using an SHMS technology. An online questionnaire survey webpage was developed using the Qualtrics platform. We launched the webpage link and handled participant recruitment using a professional agency—Prolific. Based on a statistical power analysis with G Power v3.1 software, a sample size of 208 was regarded as suitable for the complete model (Faul *et al.*, 2007). Overall, 277 valid responses were collected between October and November 2024 after filtering out incomplete and unqualified responses. The demographic information is presented in Table S4 (see the

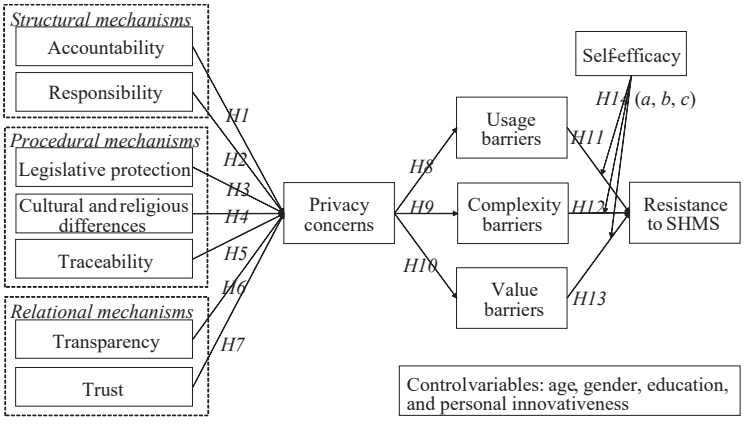

Figure 1. Concern mitigation data governance model targeting resistance to SHMSs. **Note(s):** The model includes three types of data governance mechanisms: structural (accountability, responsibility), procedural (legislative protection, cultural and religious differences, traceability), and relational (transparency, trust). **Source(s):** Authors' own work

supplementary document). The hypothesis-related measurement items were developed from sources examined in previous research (Chang and Fang, 2013; Gajanayake *et al.*, 2016; Henkens *et al.*, 2021; Karadag *et al.*, 2019; Khalil *et al.*, 2022; Khanra *et al.*, 2021; Laukkanen *et al.*, 2007; Lwin *et al.*, 2007; Mani and Chouk, 2017; ParkWerder *et al.*, 2022; Prakash and Das, 2022; Son and Kim, 2008; Trkman *et al.*, 2023; Wu *et al.*, 2021; Xu, 2019). The items are presented in Table S5 (see the supplementary document). These constructs of the model were measured via a five-point Likert scale spanning from 1 (strongly disagree) to 5 (strongly agree). All the constructs are first-order reflective constructs. The measurement and structural models were tested using Partial Least Squares-Structural Equation Modeling and SmartPLS v4 software.

3.4 Quantitative results

The model was evaluated using standard criteria for indicator reliability, internal consistency, convergent validity, and discriminant validity (Chin, 2009). After the adequacy of the measurement model, the structural model was assessed by examining collinearity among the exogenous constructs (Hair *et al.*, 2019). Table S6 (see the supplementary document) reports the final measurement results after removing items with low loadings (RESP2, CURE3, TRUS1, TRUS2, and PRIV3). Discriminant validity was examined using the Heterotrait-Monotrait (HTMT) criterion (Hair *et al.*, 2023). The HTMT values and construct correlations are reported in Table S7 and Table S8, respectively (see the supplementary document). Bootstrapping with 5,000 subsamples at a 5% significance level was used to test the significance of path coefficients (Hair *et al.*, 2019). The results of this analysis are shown in Figure 2.

The test results did not support H1 ($\beta = 0.093$, $p = 0.214$) and H2 ($\beta = 0.011$, $p = 0.907$), showing that accountability and responsibility were not significant structural data governance mechanisms affecting privacy concerns in SHMS contexts. This quantitative finding contradicts the general understanding among various stakeholder groups, especially non-consumers. However, it aligns with the minority view of consumer study participants (individual users), who paid limited attention to these structural elements during the interviews. In other words, the mechanisms related to accountability and responsibility might be significant only if individual users are engaged in policy formulation and evaluation during the development phase, rather than at the usage stage (Tallon, 2013).

The results supported H3 ($\beta = -0.211$, $p = 0.000$), showing that legislative protection was a significant procedural data governance mechanism that negatively affected privacy concerns

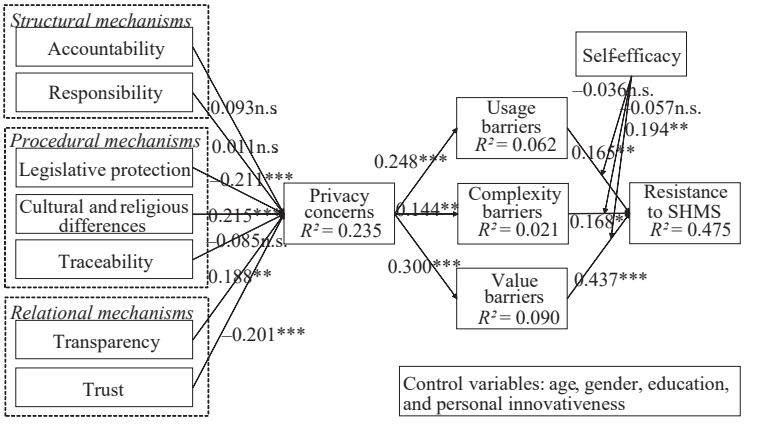

Figure 2. Structural model results. **Note(s):** *$p < 0.05$, **$p < 0.01$ and ***$p < 0.001$. **Source(s):** Authors' own work

in SHMS contexts. This result was in line with many studies that suggest a negative influence of legislative protection on customers' privacy concerns in various health informatics environments (e.g. Nguyen *et al.*, 2022; Xu, 2019). The results supported H4 ($\beta = 0.215$, $p = 0.000$), showing that cultural and religious differences were significant procedural data governance mechanisms positively affecting privacy concerns. These findings aligned with prior literature. For instance, Kulyk *et al.* (2020) confirmed the effect of cultural differences on privacy and security risk perceptions in smart health environments across three countries.

However, the results did not support H5 ($\beta = -0.085$, $p = 0.230$), showing that traceability was not a significant element affecting privacy concerns in SHMS contexts. This aligns with insights from qualitative findings and prior literature, suggesting traceability has a dual effect—it can deter counterfeiting, although it may simultaneously raise privacy concerns (Jamil *et al.*, 2020). The results supported H7 ($\beta = -0.201$, $p = 0.000$), confirming that trust had a negative impact on privacy concerns in SHMS contexts. Despite the reverse causality between trust and privacy concerns discussed in previous literature (Smith *et al.*, 2011), the findings of this study were consistent with existing literature in information systems contexts (e.g. Belanger *et al.*, 2002; Esmaeilzadeh, 2018; Fox and James, 2021). For instance, Fox and James (2021) found that users' privacy concerns decreased as trust perceptions of health technology vendors increased. However, the test results did not support H6 ($\beta = 0.188$, $p = 0.004$), as they indicated that greater transparency actually heightened privacy concerns in SHMS contexts.

The results supported H8 ($\beta = 0.248$, $p = 0.000$), H9 ($\beta = 0.144$, p = 0.009), and H10 ($\beta = 0.300$, p = 0.000). Supporting similar perspectives in existing studies (e.g. Sivakumar *et al.*, 2024; Sun *et al.*, 2024), these results suggested that privacy concerns were a significant factor that positively affected usage barriers, complexity barriers, and value barriers in relation to SHMSs. Furthermore, the test results confirmed further hypotheses: H11 ($\beta = 0.165$, $p = 0.002$), H12 ($\beta = 0.168$, $p = 0.019$), and H13 ($\beta = 0.437$, $p = 0.000$). These findings were consistent with existing studies on a wide range of new technologies. For example, Prakash and Das (2022) also found that value and complexity barriers are positively related to citizens' resistance to using digital contact tracing apps.

In addition, the results supported H14c ($\beta = 0.194$, $p = 0.004$), showing that self-efficacy moderated the effect of value barriers on users' resistance to SHMSs. Self-efficacy can be used to determine the value of technology because it influences customers' willingness to co-create value within the system (Anshu *et al.*, 2022; Bandura, 1989). However, the results did not support H14a ($\beta = -0.036$, $p = 0.537$) and H14b ($\beta = -0.057$, $p = 0.362$), indicating that self-efficacy did not moderate the effects of usage barriers and complexity barriers on users' resistance to SHMSs. This may be attributed to the fact that most survey participants reported confidence in their ability to operate SHMS devices and likely considered their usage as familiar and straightforward. Previous research has reported similar results in various digital contexts. For example, in the context of mobile applications, Kumari and Kumar (2023) found that the conditional indirect effects of usage and complexity barriers on user resistance were not significantly different between individuals with high and low self-efficacy.

The non-significant effects of age, gender, and education suggest that resistance to SHMSs may be more strongly shaped by perceived barriers and governance-related concerns than by basic demographic factors. This aligns with prior research indicating that in technology adoption contexts involving health and privacy, psychological and contextual factors often outweigh demographic influences (Kim *et al.*, 2017).

Personal innovativeness refers to an individual's willingness to try new technologies (Agarwal and Prasad, 1998), which is a key factor influencing an individual's response to technological innovations (Hong *et al.*, 2014). It plays a crucial role in determining which individuals are more likely to adopt new technologies earlier than others (Agarwal and Prasad, 1998). Building on this, we conducted a multi-group analysis (MGA) to examine the variations in level classifications of personal innovativeness and their influence on users' resistance to SHMSs.

3.4.1 Multi-group analysis. Personal innovativeness refers to an individual's willingness to try new technologies (Agarwal and Prasad, 1998), which is a key factor influencing an individual's response to technological innovations (Hong *et al.*, 2014). It plays a crucial role in determining which individuals are more likely to adopt new technologies earlier than others (Agarwal and Prasad, 1998). Building on this, we conducted a MGA to examine the variations in level classifications of personal innovativeness and their influence on users' resistance to SHMSs. MGA, a non-parametric significance test, was used to examine whether path coefficients differed between two groups (high versus low personal innovativeness with technology) were significant. Two datasets were created by grouping participants into "high" (agree/strongly agree) and "low" (disagree/strongly disagree). Given that partial measurement invariance was confirmed through the Measurement Invariance of Composite Models (MICOM), MGA was conducted following Shrout and Bolger's (2002) guidelines. The *p*-value was specifically examined to determine the significance of different group-specific path coefficients, where values < 0.50 or >0.95 indicate significant differences (Karahoca *et al.*, 2018; Sarstedt *et al.*, 2011).

The MGA results showed that several relationships were significant only for individuals with high personal innovativeness. For this group, cultural and religious differences were significantly associated with privacy concerns ($\beta = 0.258$, $p = 0.000$), and trust was also significant ($\beta = -0.211$, $p = 0.001$). Privacy concerns significantly predicted usage barriers ($\beta = 0.288$, $p = 0.000$) and complexity barriers ($\beta = 0.154$, $p = 0.009$). Both usage barriers ($\beta = 0.172$, $p = 0.003$) and complexity barriers ($\beta = 0.194$, $p = 0.012$) significantly increased resistance to SHMS. Self-efficacy moderated the effect of value barriers on resistance ($\beta = 0.204$, $p = 0.002$). None of these relationships were significant for the low-innovative group.

4. Discussion

Drawing on innovation resistance theory and data governance mechanisms, the study employed a developmental mixed-methods research approach. The qualitative findings from Study 1 suggest that seven salient elements of data governance mechanisms influence users' privacy concerns in relation to users' resistance to SHMSs: *accountability*, *responsibility*, *legislative protection*, *cultural and religious differences*, *traceability*, *transparency*, and *trust*. Although Study 1 identified seven key elements through qualitative inquiry, only a subset demonstrated statistical significance in Study 2. This does not indicate a lack of rigor in the qualitative phase. Instead, it reflects the nuanced distinction between perceived relevance (qualitative insight) and statistically significant predictive power (quantitative validation). The development of our model was still rather exploratory, and the individual factors within the model derived from interview data were not guaranteed to be empirically salient when tested as part of a full model. Thus, the inclusion of non-significant constructs ensures model completeness and strengthens our theoretical contributions by identifying boundary conditions for each governance mechanism's effect. The findings in Study 1 also support the relationships between privacy concerns and functional barriers that ultimately influence users' resistance to SHMSs. Based on these qualitative findings, in Study 2, we developed a research model and quantitatively tested it. Guided by Venkatesh *et al.* (2013, 2016), three meta-inferences were extracted that represent an integration of the findings of the entire study.

4.1 Meta inferences and theoretical implications

4.1.1 Meta-inference 1: procedural data governance is the most effective mechanism for immediate resistance reduction in the use of SHMSs through its legislative, cultural, and religious aspects. The study indicates that procedural data governance mechanisms including legislative protection and cultural and religious sensitivity, have a notably more substantial impact on mitigating user resistance to the use of SHMSs. In contrast, structural mechanisms like accountability and responsibility have a lesser effect. This finding contradicts existing

studies in various digital contexts that highlight the direct impact of structural mechanisms in reducing privacy concerns. This divergence arises because of prior studies' focus on general digital contexts (e.g. general e-commerce or smart services), where users have broader expectations of long-term organizational transparency and compliance.

In contrast, SHMSs deal with highly sensitive health data, requiring immediate and visible reassurances to address unique user anxieties tied to privacy and ethical data handling. This shifts the emphasis from structural trust mechanisms to procedural safeguards that offer direct, contextually relevant solutions. For instance, Elahi *et al.* (2019) argued that accountability mechanisms are crucial for protecting the privacy of smart service users as they ensure users are not deceived and violated. Kayhan and Davis (2016) suggested that a service provider's responsibility for a violation (e.g. a data breach) is an influential element associated with privacy concerns. However, in the smart health context, accountability and responsibility elements often remain invisible, but can be brought to light through regulatory enforcement, such as punitive measures outlined in the GDPR (Elahi *et al.*, 2019; Sivakumar *et al.*, 2024). This invisibility stems from the reactive nature of structural mechanisms, which only becomes apparent after incidents (e.g. data breaches) happen. SHMS users, however, require proactive assurances to alleviate their initial fears about data misuse (Haggag *et al.*, 2022). Aligned with these considerations, the lack of significant effects as shown in our findings suggests that accountability and responsibility are perceived as more institutional-level or abstract constructs. Users might not directly associate with their personal experience of privacy risk. These structural mechanisms may only become salient when users are involved in governance processes or aware of specific breaches (Tallon, 2013). As such, their perceived relevance may be limited during routine SHMS use. Instead, procedural mechanisms fulfill this need by offering clear and perceivable actions that instill confidence before any incident happens, making them more immediately effective.

Procedural governance directly addresses privacy concerns by establishing and implementing clear, actionable safeguards and guidelines for data use that are readily perceivable by users. This direct impact builds confidence among users in terms of their data privacy and security, effectively mitigating any psychological and functional barriers to adopting SHMSs. In SHMS adoption, where the stakes involve personal health data, immediate trust is paramount. Procedural mechanisms such as legislative protections and culturally sensitive practices provide users with an assurance of safety and ethical treatment, overcoming the psychological hurdles that often prevent engagement with health monitoring systems. Therefore, procedural governance mechanisms provide an immediate, visible means to lower resistance by empowering users with a sense of control and a clear understanding of data handling practices.

The non-significant relationship between traceability and privacy concerns shown in the findings may be due to the ambivalent nature of traceability. While traceability mechanisms are often designed to enhance security and system integrity, they may also increase user awareness of continuous surveillance and data tracking. This duality—also observed in prior work (Jamil *et al.*, 2020)—could lead users to view traceability as both protective and intrusive, thereby weakening its net impact on privacy concerns.

While legislative protection and cultural/religious sensitivity emerged as significant procedural mechanisms in mitigating privacy concerns, it is important to recognize that their effectiveness may vary depending on the maturity of the SHMS ecosystem. In early-stage or pilot deployments—like those common in current settings—regulatory frameworks may still be evolving, and users may not yet fully perceive long-term governance practices. Additionally, traceability, although theoretically positioned as a privacy-enhancing feature, was not supported in our model. This suggests that users may not view traceability as beneficial at this stage, potentially due to limited transparency about its implementation, or concerns that such monitoring could actually increase perceived surveillance. As SHMS platforms mature and trust in system-level safeguards grows, the role of these mechanisms may also shift.

4.1.2 Relational mechanisms and their role are influential in long-term resistance reduction through trust. Relational data governance mechanisms, particularly trust, are found to be more influential than structural mechanisms in fostering acceptance of SHMSs. While procedural mechanisms provide immediate assurance, relational mechanisms help build sustained confidence by fostering trust over time (Borgman *et al.*, 2016; DAMA International, 2009). This distinction is because procedural mechanisms focus on short-term, visible safeguards that address immediate user concerns, whereas relational mechanisms operate through repeated interactions and user engagement over time (Hernandez-Ortega *et al.*, 2022). This approach fosters deeper psychological comfort and ongoing acceptance, which is particularly important for SHMSs that require consistent user participation.

Unlike structural mechanisms, which typically focus on accountability after incidents or violations, relational mechanisms proactively engage users by communicating the value and security of their participation. This proactive engagement fosters a sense of partnership and collaboration, which is essential for sustaining long-term trust. These mechanisms concentrate on increased knowledge and understanding as well as clear communication of mutual benefits among stakeholders (Frangopoulou *et al.*, 2024; Vigurs *et al.*, 2021). In other words, trust-focused mechanisms foster mutual understanding and real collaboration among stakeholders toward shared goals (Chatfield and AlAnazi, 2015). This collaborative approach is critical in the SHMS context, where users may initially feel vulnerable due to the sensitive nature of their health data. By addressing these vulnerabilities through relational mechanisms, SHMS providers can encourage long-term usage and engagement. The findings align with previous research highlighting the importance of trust-building strategies in addressing privacy concerns in various health information technologies (e.g. Lambillotte *et al.*, 2022; Oulasvirta *et al.*, 2014; Trkman *et al.*, 2023; Xu, 2019). Therefore, structural mechanisms typically operate at an organizational level with limited direct visibility amongst users. In contrast, relational governance engages users on a personal level through long-term repeated interactions. This makes it a critical factor for sustained SHMS adoption and usage. This long-term focus ensures that relational mechanisms go beyond reactive enforcement and instead foster ongoing relationships between users and providers, which improves trust over time.

While relational governance mechanisms such as trust are found to play a significant role in reducing resistance over time, the role of transparency appears to be more complex. Contrary to expectations, our results show that greater transparency is associated with increased privacy concerns. Transparency is generally assumed to build trust and lessen uncertainty. However, too much transparency or presenting it ineffectively can have the opposite effect. When users are exposed to detailed information about how their data is collected, stored, or shared—especially in highly sensitive health contexts—they may become more conscious of the risks involved (Xu, 2019). In such cases, transparency may amplify rather than alleviate privacy concerns, particularly if it reveals complex data flows or broad third-party access. This aligns with findings in prior research suggesting that too much transparency without adequate reassurance or user control can result in information overload or heightened risk perception (Elahi *et al.*, 2019; Mabillard *et al.*, 2021). Moreover, privacy perception is sometimes highly individualized, varying across users with different privacy predispositions, so the impact of transparency largely depends on individual preferences (Awad and Krishnan, 2006; Bemmann *et al.*, 2022). Therefore, transparency must be carefully designed—not simply to inform, but to empower and reassure users—especially in high-stakes domains like SHMSs.

4.1.3 Privacy concerns indirectly contribute to user resistance to SHMSs that have been transformed into multipliers for functional barriers. Our findings show that while privacy concerns alone may not directly cause users to reject SHMSs, they significantly contribute to resistance by intensifying functional barriers related to usability, complexity, and perceived value. This finding differs from previous studies that position privacy concerns as direct predictors of user resistance (e.g. Kaur *et al.*, 2020; Prakash and Das, 2022). This difference may be because of the unique dynamics of SHMSs, where privacy anxieties often manifest indirectly, amplifying other barriers, such as the perceived difficulty of using the system or

doubts about its benefits. For instance, anxiety over data privacy often translates into heightened sensitivity toward the complexity and perceived risks associated with SHMSs (Deutsch *et al.*, 2011; Galvin and DeMuro, 2020). Users' psychological preoccupation with data misuse or lack of control may make even well-designed SHMSs appear overly complex or intimidating (Wilson *et al.*, 2021). This psychological lens highlights the importance of addressing privacy indirectly through usability-focused measures. Privacy concerns can lead users to view data-sharing requirements as overly complicated or intrusive, which, in turn, diminishes the perceived value of the system (e.g. Hubert *et al.*, 2019; Shaw and Sergueeva, 2019). This cascading effect transforms privacy concerns into a multiplier for other barriers rather than an isolated resistance factor. As a result, these systems are perceived as more burdensome and less beneficial, indirectly fueling users' resistance to SHMSs.

Recognizing privacy concerns as an underlying contributor to functional barriers underscores the need for targeted strategies to reduce user resistance. Effective data governance practices, such as robust legislative protections and transparent data handling practices, can help alleviate complexity-related barriers. For example, transparency mechanisms, such as providing users with clear, comprehensible privacy policies and demonstrating security measures, can bridge the gap between user anxiety and functional understanding. By addressing privacy concerns, organizations can minimize perceptions of system complexity and highlight an SHMS'susability and value. This proactive approach can not only lower resistance but also reshape the user experience, turning privacy management into an enabler, rather than a constraint.

In summary, this study advances the current understanding of innovation resistance by incorporating data governance, illustrating how innovation resistance theory can be adapted to meet the varied demands of the HIT sector. It contributes by highlighting the unique challenges that SHMSs face in handling highly sensitive health data, challenges that necessitate immediate, visible reassurances to ease user concerns about privacy and ethical data use. In contrast, emphasizing long-term relational strategies supports ongoing engagement between users and providers, fostering trust gradually through sustained interaction rather than solely through reactive measures.

4.2 Implications for practice and society

This study serves as a valuable resource for practical applications. It builds upon innovation resistance theory by integrating data governance, demonstrating how theoretical models can be tailored to address diverse needs within the HIT domain. Our findings show that cultural and religious differences significantly influence privacy concerns, reinforcing the importance of context-aware policy design. Policymakers and healthcare institutions should develop culturally responsive data-sharing protocols, including localized consent models, multilingual interfaces, and sensitivity to gender norms in healthcare delivery (Karadag *et al.*, 2019). These adjustments can reduce procedural friction and help users feel more respected and protected when using SHMSs. Understanding these differences (e.g. digital literacy among diverse groups/cultures) can guide the development of user interfaces and support systems that are culturally and linguistically adapted to meet the specific needs of diverse user groups, thus reducing perceived complexity. Cultural and religious considerations should be integrated into the procedural aspects of data governance. For instance, healthcare providers could implement customized consent forms and privacy notices aligned with cultural norms surrounding information sharing in order to enhance trust. This would show respect for the user's cultural background, which can be crucial for systems like SHMSs that handle sensitive personal health data. This level of customization would not only mitigate privacy concerns but also address potential resistance due to cultural mismatches.

Given the significant role of trust as a relational mechanism, providers must prioritize long-term engagement strategies that go beyond compliance. These may include transparent explanations of data practices accompanied by user control options, ongoing user education,

and personalized support. Additionally, based on the results of our MGA, communication strategies should be tailored to users' levels of personal innovativeness, ensuring that both early adopters and more hesitant users feel confident and informed. Healthcare providers and technology providers can leverage insights from this study to collaboratively develop effective communication strategies that address privacy concerns based on various levels of personal innovativeness. When developing data governance policies, government authority policy makers can also consider the differential impacts on groups in relation to their personal innovativeness. Policies should not only be equitable but also sufficiently flexible to address these varied impacts effectively. For instance, insights regarding procedural mechanisms can be applied in regions with different regulatory and cultural contexts.

The findings that self-efficacy significantly moderates the effect of value barriers on users' resistance highlights a critical insight for healthcare providers: building user confidence in SHMS technology can reduce perceived value-related concerns and, ultimately, resistance. Practical strategies might include onboarding tutorials, live demonstrations, and personalized user support to boost perceived self-efficacy. In addition, the MGA revealed that data governance mechanisms were less effective for users with low personal innovativeness. This suggests that a "one-size-fits-all" approach to policy communication or system design may fall short for more hesitant users. Practically, SHMS providers could consider simple screening tools (e.g. short surveys) to assess innovativeness levels and deliver differentiated support—such as more guided onboarding or community-based engagement strategies—for users less open to new technologies.

Beyond practical applications, the findings of this study carry important societal implications. By highlighting how data governance mechanisms—particularly procedural and relational mechanisms—affect users' privacy concerns and resistance, this research contributes to shaping public attitudes toward trust and transparency in digital health systems. For example, the significance of cultural and religious differences suggests that SHMS implementation must be culturally adaptive. In regions with strong religious norms or diverse linguistic populations (e.g. Middle Eastern countries or multilingual Asian societies), procedural adjustments (e.g. culturally tailored consent models or language-localized user interfaces) can improve acceptance. In terms of regulatory diversity, countries with weaker legislative frameworks (e.g. emerging markets with limited data protection laws) may need to rely more on relational trust-building strategies—such as visible provider commitments and community engagement—to reduce privacy concerns in the absence of robust formal protections. Over the long term, these insights can guide policy development to ensure that SHMS platforms evolve alongside appropriate privacy safeguards, inclusive design practices, and trust-enhancing governance structures.

5. Conclusions, limitations, and future directions

Drawing on innovation resistance theory and data governance mechanisms, this mixed-method study explored the elements contributing to resistance to SHMSs and how data governance mechanisms influence individuals' concerns and barriers. We proposed a concern mitigation data governance model to address SHMS users' resistance and offered actionable insights for healthcare providers, technology providers, and policymakers. This study has several limitations, including the potential for sample selection bias. Because the data were collected in New Zealand and Australia, they may reflect regional or cultural factors, such as trust in government, health system structures, or privacy rules, that may not be generalizable to other regions. Future research should examine how data governance influences privacy concerns and resistance across different cultural, institutional, and regulatory contexts. Future research could validate the proposed model in non-Western contexts, where differences in regulatory maturity and cultural expectations around health data may yield distinct patterns of resistance.

Further studies could apply the model to other health monitoring technologies (e.g. mental health and wellbeing apps, remote rehabilitation systems, and telemedicine platforms) to

examine whether similar governance and resistance dynamics emerge across different contexts. It would be beneficial to explore whether privacy concerns have a direct effect on user resistance, beyond their indirect influence through other barriers. This study surveyed only individual users. Future research could include other stakeholders, such as healthcare professionals and technology providers, for a fuller view of SHMS resistance and adoption. It should also examine the experiences of actual SHMS users, not just potential ones.

Acknowledgments

This study was approved by the institute's Research Ethics Committee, with reference number 22/156. This paper is an extended and revised version of a study originally presented in the proceedings of the Australasian Conference on Information Systems (ACIS) 2024. Supplementary material for this article is available online.

Supplementary material

The supplementary material for this article can be found online.

References

Abraham, R., Schneider, J. and Vom Brocke, J. (2019), "Data governance: a conceptual framework, structured review, and research agenda", *International Journal of Information Management*, Vol. 49, pp. 424-438, doi: 10.1016/j.ijinfomgt.2019.07.008.

Accenture.com (2020), "How can leaders make recent digital health gains last?", available at: https://www.accenture.com/us-en/insights/health/leaders-make-recent-digital-health-gains-last (accessed 26 April 2024).

Agarwal, R. and Prasad, J. (1998), "A conceptual and operational definition of personal innovativeness in the domain of information technology", *Information Systems Research*, Vol. 9 No. 2, pp. 204-215, doi: 10.1287/isre.9.2.204.

Almujally, N.A., Aljrees, T., Saidani, O., Umer, M., Faheem, Z.B., Abuzinadah, N., Alnowaiser, K. and Ashraf, I. (2023), "Monitoring acute heart failure patients using internet-of-things-based smart monitoring system", *Sensors*, Vol. 23 No. 10, 4580, doi: 10.3390/s23104580.

Alsamhi, S.H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., Wei, X., Guizan, M. and Curry, E. (2024), "Federated learning meets blockchain in decentralized data sharing: Healthcare use case", *IEEE Internet of Things Journal*, Vol. 11 No. 11, pp. 19602-19615, doi: 10.1109/JIOT.2024.3367249.

Anshu, K., Shankar, A., Behl, A., Pereira, V. and Laker, B. (2022), "Impact of barriers of value co-creation on consumers' innovation resistance behavior: investigating the moderation role of the DART model", *Technological Forecasting and Social Change*, Vol. 184, 122033, doi: 10.1016/j.techfore.2022.122033.

Awad, N.F. and Krishnan, M.S. (2006), "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization", *MIS Quarterly*, Vol. 30 No. 1, pp. 13-28, doi: 10.2307/25148715.

Bandura, A. (1989), "Regulation of cognitive processes through perceived self-efficacy", *Developmental Psychology*, Vol. 25 No. 5, pp. 729-735, doi: 10.1037/0012-1649.25.5.729.

Bélanger, F. and Crossler, R.E. (2011), "Privacy in the digital age: a review of information privacy research in information systems", *MIS Quarterly*, Vol. 35 No. 4, pp. 1017-1041, doi: 10.2307/41409971.

Belanger, F., Hiller, J.S. and Smith, W.J. (2002), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", *The Journal of Strategic Information Systems*, Vol. 11 No. 3, pp. 245-270, doi: 10.1016/S0963-8687(02)00018-5.

Bemmann, F., Windl, M., Erbe, J., Mayer, S. and Hussmann, H. (2022), "The influence of transparency and control on the willingness of data sharing in adaptive mobile apps", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6 MHCI, pp. 1-26.

Borgman, H., Heier, H., Bahli, B. and Boekamp, T. (2016), "Dotting the I and crossing (out) the T in IT governance: new challenges for information governance", *2016 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: 10.1191/1478088706qp063oa.

Capterra.com (2021), "New technologies for telehealth in Canada: 61% of Canadians want to implement AI", available at: https://www.capterra.ca/blog/2039/telehealth-in-canada-technology-ai (accessed 25 November 2025).

Chang, Y. and Fang, S. (2013), "Antecedents and distinctions between online trust and distrust: predicting high-and low-risk internet behaviors", *Journal of Electronic Commerce Research*, Vol. 14 No. 2, pp. 149-166.

Chatfield, A.T. and AlAnazi, J. (2015), "Collaborative governance matters to e-government interoperability: an analysis of citizen-centric integrated interoperable e-government implementation in Saudi Arabia", *International Journal of Public Administration in the Digital Age (IJPADA)*, Vol. 2 No. 3, pp. 24-44, doi: 10.4018/ijpada.2015070102.

Chibuike, M.C., Sara, G.S. and Adele, B. (2024), "Overcoming challenges for improved patient-centric care: a scoping review of platform ecosystems in healthcare", *IEEE Access*, Vol. 12, pp. 14298-14313, doi: 10.1109/ACCESS.2024.3356860.

Chin, W.W. (2009), "How to write up and report PLS analyses", in Esposito Vinzi, V., Chin, W.W., Henseler, J. and Wang, H. (Eds), *Handbook of Partial Least Squares: Concepts, Methods and Applications*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 655-690.

Chouk, I. and Mani, Z. (2019), "Factors for and against resistance to smart services: role of consumer lifestyle and ecosystem related variables", *Journal of Services Marketing*, Vol. 33 No. 4, pp. 449-462, doi: 10.1108/JSM-01-2018-0046.

Clarke, R. (2019), "Risks inherent in the digital surveillance economy: a research agenda", *Journal of Information Technology*, Vol. 34 No. 1, pp. 59-80, doi: 10.1177/0268396218815559.

Coert, R.M.H., Timmis, J.K., Boorsma, A. and Pasman, W.J. (2021), "Stakeholder perspectives on barriers and facilitators for the adoption of virtual clinical trials: qualitative Study", *Journal of Medical Internet Research*, Vol. 23 No. 7, e26813, doi: 10.2196/26813.

Creswell, J.W. and Plano Clark, V.L. (2018), *Designing and Conducting Mixed Methods Research*, 3rd ed., Sage, Los Angeles.

Creswell, J.W. and Poth, C.N. (2018), *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 4th ed., Sage, Los Angeles, CA.

Crossler, R.E. and Bélanger, F. (2019), "Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap", *Information Systems Research*, Vol. 30 No. 3, pp. 995-1006, doi: 10.1287/isre.2019.0846.

Dahlsrud, A. (2008), "How corporate social responsibility is defined: an analysis of 37 definitions", *Corporate Social Responsibility and Environmental Management*, Vol. 15 No. 1, pp. 1-13, doi: 10.1002/csr.132.

DAMA International (2009), *The DAMA Guide to the Data Management Body of Knowledge*, 1st ed., Technics Publications, LLC., NJ.

Davidson, E., Wessel, L., Winter, J.S. and Winter, S. (2023), "Future directions for scholarship on data governance, digital innovation, and grand challenges", *Information and Organization*, Vol. 33 No. 1, 100454, doi: 10.1016/j.infoandorg.2023.100454.

Deutsch, M., Coleman, P.T. and Marcus, E.C. (2011), *The Handbook of Conflict Resolution: Theory and Practice*, John Wiley & Sons, San Francisco, CA.

Dhagarra, D., Goswami, M. and Kumar, G. (2020), "Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective", *International Journal of Medical Informatics*, Vol. 141, pp. 1-13, doi: 10.1016/j.ijmedinf.2020.104164.

Duckert, M. and Barkhuus, L. (2022), "Protecting personal health data through privacy awareness: a study of perceived data privacy among people with chronic or long-term illness", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6 GROUP, pp. 1-22, doi: 10.1145/3492830.

Eagleson, R., Altamirano-Diaz, L., McInnis, A., Welisch, E., De Jesus, S., Prapavessis, H., Rombeek, M., Seabrook, J.A., Park, T. and Norozi, K. (2017), "Implementation of clinical research trials using web-based and mobile devices: challenges and solutions", *BMC Medical Research Methodology*, Vol. 17, pp. 1-8, doi: 10.1186/s12874-017-0324-6.

Ebrahim, A.H. and Buheji, M. (2020), "A pursuit for a 'holistic social responsibility strategic framework' addressing COVID-19 pandemic needs", *American Journal of Economics*, Vol. 10 No. 5, pp. 293-304, doi: 10.5923/j.economics.20201005.04.

Elahi, H., Wang, G., Peng, T. and Chen, J. (2019), "On transparency and accountability of smart assistants in smart cities", *Applied Sciences*, Vol. 9 No. 24, pp. 1-26, doi: 10.3390/app9245344.

Esmaeilzadeh, P. (2018), "Healthcare consumers' opt-in intentions to health information exchanges (HIEs): an empirical study", *Computers in Human Behavior*, Vol. 84, pp. 114-129, doi: 10.1016/j.chb.2018.02.029.

Faul, F., Erdfelder, E., Lang, A.-G. and Buchner, A. (2007), "G* power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences", *Behavior Research Methods*, Vol. 39 No. 2, pp. 175-191, doi: 10.3758/BF03193146.

Fortune.com (2023), "The best technology to prevent falls, monitor safety, and help older adults age in place longer", available at: https://fortune.com/well/2023/02/03/technology-can-help-older-adults-age-in-place-longer/ (accessed 25 November 2025).

Fox, A.K. and Hoy, M.G. (2019), "Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: an investigation of mothers", *Journal of Public Policy and Marketing*, Vol. 38 No. 4, pp. 414-432, doi: 10.1177/0743915619858290.

Fox, G. and James, T.L. (2021), "Toward an understanding of the antecedents to health information privacy concern: a mixed methods study", *Information Systems Frontiers*, Vol. 23 No. 6, pp. 1537-1562, doi: 10.1007/s10796-020-10053-0.

Frangopoulou, M., van der Laan, L. and Ebbers, W. (2024), "The privacy calculus in the context of novel health technology for diagnosing and tracking infectious diseases: the role of disease severity and technology's evidence base for effectiveness in adoption and voluntary health data-sharing", *Technology in Society*, Vol. 78, 102616, doi: 10.1016/j.techsoc.2024.102616.

Friedman, N. and Ormiston, J. (2022), "Blockchain as a sustainability-oriented innovation?: opportunities for and resistance to blockchain technology as a driver of sustainability in global food supply chains", *Technological Forecasting and Social Change*, Vol. 175, 121403, doi: 10.1016/j.techfore.2021.121403.

Gajanayake, R., Iannella, R. and Sahama, T. (2016), "An insight into the adoption of Accountable-eHealth systems – an empirical research model based on the Australian context", *Innovation and Research in BioMedical Engineering*, Vol. 37 No. 4, pp. 219-231, doi: 10.1016/j.irbm.2016.01.002.

Galvin, H.K. and DeMuro, P.R. (2020), "Developments in privacy and data ownership in Mobile health technologies, 2016-2019", *IMIA Yearbook of Medical Informatics*, Vol. 29 No. 01, pp. 32-43, doi: 10.1055/s-0040-1701987.

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J. and Vayena, E. (2020), "Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid", *The Lancet Digital Health*, Vol. 2 No. 8, pp. e425-e434, doi: 10.1016/S2589-7500(20)30137-0.

Glaser, B.G. and Strauss, A.L. (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Adline de Gruyter, New York.

GlobeNewswire (2023), "Smart Medical devices market expecting to hit USD 474 billion by 2032, with a CAGR of 12.3 %", available at: https://www.globenewswire.com/news-release/2023/12/13/2795357/0/en/Smart-Medical-Devices-Market-Expecting-to-Hit-USD-474-Billion-by-2032-with-a-CAGR-of-12-3-Market-us.html

Haggag, O., Grundy, J., Abdelrazek, M. and Haggag, S. (2022), "A large scale analysis of mHealth app user reviews", *Empirical Software Engineering*, Vol. 27 No. 7, p. 196, doi: 10.1007/s10664-022-10222-6.

Hair, J., Hair, J.F., Jr., Sarstedt, M., Ringle, C.M. and Gudergan, S.P. (2023), *Advanced Issues in Partial Least Squares Structural Equation Modeling*, Sage, Thousand Oaks, CA.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24, doi: 10.1108/EBR-11-2018-0203.

Harris, J.E. (2020), "Taking disability public", *University of Pennsylvania Law Review*, Vol. 169, pp. 1681-1749.

Henkens, B., Verleye, K. and Larivière, B. (2021), "The smarter, the better?! customer well-being, engagement, and perceptions in smart service systems", *International Journal of Research in Marketing*, Vol. 38 No. 2, pp. 425-447, doi: 10.1016/j.ijresmar.2020.09.006.

Hernandez-Ortega, B., Aldas-Manzano, J. and Ferreira, I. (2022), "Relational cohesion between users and smart voice assistants", *Journal of Services Marketing*, Vol. 36 No. 5, pp. 725-740, doi: 10.1108/JSM-07-2020-0286.

Hew, J.-J., Leong, L.-Y., Tan, G.W.-H., Ooi, K.-B. and Lee, V.-H. (2019), "The age of mobile social commerce: an Artificial neural network analysis on its resistances", *Technological Forecasting and Social Change*, Vol. 144, pp. 311-324, doi: 10.1016/j.techfore.2017.10.007.

Hong, W., Chan, F.K., Thong, J.Y., Chasalow, L.C. and Dhillon, G. (2014), "A framework and guidelines for context-specific theorizing in information systems research", *Information Systems Research*, Vol. 25 No. 1, pp. 111-136, doi: 10.1287/isre.2013.0501.

Hubert, M., Blut, M., Brock, C., Zhang, R.W., Koch, V. and Riedl, R. (2019), "The influence of acceptance and adoption drivers on smart home usage", *European Journal of Marketing*, Vol. 53 No. 6, pp. 1073-1098, doi: 10.1108/EJM-12-2016-0794.

Hunter, I., Elers, P., Lockhart, C., Guesgen, H., Singh, A. and Whiddett, D. (2020), "Issues associated with the management and governance of sensor data and information to assist aging in place: focus group study with health care professionals", *JMIR mHealth and uHealth*, Vol. 8 No. 12, pp. 1-10, doi: 10.2196/24157.

Ismail, L., Materwala, H., Karduck, A.P. and Adem, A. (2020), "Requirements of health data management systems for biomedical care and research: scoping review", *Journal of Medical Internet Research*, Vol. 22 No. 7, e17508, doi: 10.2196/17508.

Iyanna, S., Kaur, P., Ractham, P., Talwar, S. and Najmul Islam, A.K.M. (2022), "Digital transformation of healthcare sector. What is impeding adoption and continued usage of technology-driven innovations by end-users?", *Journal of Business Research*, Vol. 153, pp. 150-161, doi: 10.1016/j.jbusres.2022.08.007.

Jamil, F., Ahmad, S., Iqbal, N. and Kim, D.H. (2020), "Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals", *Sensors*, Vol. 20 No. 8, pp. 1-26, doi: 10.3390/s20082195.

Janssen, M., Brous, P., Estevez, E., Barbosa, L.S. and Janowski, T. (2020), "Data governance: organizing data for trustworthy artificial intelligence", *Government Information Quarterly*, Vol. 37 No. 3, 101493, doi: 10.1016/j.giq.2020.101493.

Karadag, E., Parlar Kilic, S., Ugur, O. and Akyol, M.A. (2019), "Attitudes of nurses in Turkey toward care of dying individual and the associated religious and cultural factors", *Journal of Religion and Health*, Vol. 58 No. 1, pp. 303-316, doi: 10.1007/s10943-018-0657-4.

Karahoca, A., Karahoca, D. and Aksöz, M. (2018), "Examining intention to adopt to internet of things in healthcare technology products", *Kybernetes*, Vol. 47 No. 4, pp. 742-770, doi: 10.1108/K-02-2017-0045.

Kaur, P., Dhir, A., Singh, N., Sahu, G. and Almotairi, M. (2020), "An innovation resistance theory perspective on Mobile payment solutions", *Journal of Retailing and Consumer Services*, Vol. 55, 102059, doi: 10.1016/j.jretconser.2020.102059.

Kayhan, V.O. and Davis, C.J. (2016), "Situational privacy concerns and antecedent factors", *Journal of Computer Information Systems*, Vol. 56 No. 3, pp. 228-237, doi: 10.1080/08874417.2016.1153913.

Khalil, A., Shankar, A., Bodhi, R., Behl, A. and Ferraris, A. (2022), "Why do people resist drone food delivery services? An innovation resistance theory perspective", *IEEE Transactions on Engineering Management*, Vol. 71, pp. 13038-13048, doi: 10.1109/TEM.2022.3202485.

Khanra, S., Dhir, A., Kaur, P. and Joseph, R.P. (2021), "Factors influencing the adoption postponement of mobile payment services in the hospitality sector during a pandemic", *Journal of Hospitality and Tourism Management*, Vol. 46, pp. 26-39, doi: 10.1016/j.jhtm.2020.11.004.

Kim, B., Hong, S. and Cameron, G.T. (2014), "What corporations say matters more than what they say they do? A test of a truth claim and transparency in press releases on corporate websites and Facebook pages", *Journalism and Mass Communication Quarterly*, Vol. 91 No. 4, pp. 811-829, doi: 10.1177/1077699014550087.

Kim, Y., Park, Y. and Choi, J. (2017), "A study on the adoption of IoT smart home service: using Value-based adoption model", *Total Quality Management and Business Excellence*, Vol. 28 Nos 9/10, pp. 1149-1165, doi: 10.1080/14783363.2017.1310708.

Knoppers, B.M. and Thorogood, A.M. (2017), "Ethics and big data in health", *Current Opinion in Systems Biology*, Vol. 4, pp. 53-57, doi: 10.1016/j.coisb.2017.07.001.

Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N. and Volkamer, M. (2020), *Security and Privacy Awareness in Smart Environments–a Cross-country Investigation, Proceedings of Asiausec 2020, Financial Cryptography and Data Security*, Springer, Sabah.

Kumari, P. and Kumar, A. (2023), "Investigating the dark side of mobile bookkeeping applications: a moderated-mediation approach", *VINE Journal of Information and Knowledge Management Systems*, Vol. 53 No. 5, pp. 985-1004, doi: 10.1108/VJIKMS-09-2022-0298.

Lambillotte, L., Bart, Y. and Poncin, I. (2022), "When does information transparency reduce downside of personalization? Role of need for cognition and perceived control", *Journal of Interactive Marketing*, Vol. 57 No. 3, pp. 393-420, doi: 10.1177/10949968221095557.

Laukkanen, T., Sinkkonen, S., Kivijärvi, M. and Laukkanen, P. (2007), "Innovation resistance among mature consumers", *Journal of Consumer Marketing*, Vol. 24 No. 7, pp. 419-427, doi: 10.1108/07363760710834834.

Lewis, D. and Moorkens, J. (2020), "A rights-based approach to trustworthy AI in social media", *Social Media + Society*, Vol. 6 No. 3, 2056305120954672, doi: 10.1177/2056305120954672.

Li, X., Zhou, Y., Liu, Y., Wang, X. and Yuen, K.F. (2023), "Psychological antecedents of telehealth acceptance: a technology readiness perspective", *International Journal of Disaster Risk Reduction*, Vol. 91, pp. 1-12, doi: 10.1016/j.ijdrr.2023.103688.

Lomotey, R.K., Pry, J. and Sriramoju, S. (2017), "Wearable IoT data stream traceability in a distributed health information system", *Pervasive and Mobile Computing*, Vol. 40, pp. 692-707, doi: 10.1016/j.pmcj.2017.06.020.

Lwin, M., Wirtz, J. and Williams, J.D. (2007), "Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective", *Journal of the Academy of Marketing Science*, Vol. 35 No. 4, pp. 572-585, doi: 10.1007/s11747-006-0003-3.

Mabillard, V., Demartines, N. and Joliat, G.-R. (2021), "How can reasoned transparency enhance co-creation in healthcare and remedy the pitfalls of digitization in doctor-patient relationships?", *International Journal of Health Policy and Management*, Vol. 11 No. 10, pp. 1986-1990, doi: 10.34172/ijhpm.2020.263.

Maddah, M., Esmaeilzadeh, P. and Mirzaei, T. (2024), "An experimental study to examine relationships between IT identity and users' post-adoption behaviors for different types of health applications", *Information Systems Management*, Vol. 41 No. 3, pp. 238-264, doi: 10.1080/10580530.2023.2237187.

Mani, Z. and Chouk, I. (2017), "Drivers of consumers' resistance to smart products", *Journal of Marketing Management*, Vol. 33 Nos 1/2, pp. 76-97, doi: 10.1080/0267257X.2016.1245212.

Mani, Z. and Chouk, I. (2018), "Consumer resistance to innovation in services: challenges and barriers in the internet of things era", *Journal of Product Innovation Management*, Vol. 35 No. 5, pp. 780-807, doi: 10.1111/jpim.12463.

Market.Us (2023), "Global smart medical devices market", available at: https://market.us/report/smart-medical-devices-market/ (accessed 16 September 2025).

Matt, C., Becker, M., Kolbeck, A. and Hess, T. (2019), "Continuously healthy, continuously used?–A thematic analysis of user perceptions on consumer health wearables", *Pacific Asia Journal of the Association for Information Systems*, Vol. 11 No. 1, pp. 108-132, doi: 10.17705/1pais.11105.

Mensah, I.K., Zeng, G. and Mwakapesa, D.S. (2022), "The behavioral intention to adopt mobile health services: the moderating impact of mobile self-efficacy", *Frontiers in Public Health*, Vol. 10, pp. 1-14, doi: 10.3389/fpubh.2022.1020474.

Nguyen, T.T., Tran Hoang, M.T. and Phung, M.T. (2022), "To our health! perceived benefits offset privacy concerns in using national contact-tracing apps", *Library Hi Tech*, Vol. 41 No. 1, pp. 174-191, doi: 10.1108/LHT-12-2021-0461.

Nissenbaum, H. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA.

Okazaki, S., Castañeda, J.A., Sanz, S. and Henseler, J. (2013), "Physicians' appraisal of mobile health monitoring", *Service Industries Journal*, Vol. 33 Nos 13-14, pp. 1326-1344, doi: 10.1080/02642069.2013.815737.

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A. and Karvonen, K. (2014), "Transparency of intentions decreases privacy concerns in ubiquitous surveillance", *Cyberpsychology, Behavior, and Social Networking*, Vol. 17 No. 10, pp. 633-638, doi: 10.1089/cyber.2013.0585.

Pal, D., Funilkul, S. and Papasratorn, B. (2019), "Antecedents of trust and the continuance intention in IoT-based smart products: the case of consumer wearables", *IEEE Access*, Vol. 7, pp. 184160-184171, doi: 10.1109/ACCESS.2019.2960467.

Park, E.H., Werder, K., Cao, L. and Ramesh, B. (2022), "Why do family members reject AI in health care? Competing effects of emotions", *Journal of Management Information Systems*, Vol. 39 No. 3, pp. 765-792, doi: 10.1080/07421222.2022.2096550.

Park, I., Kim, D., Moon, J., Kim, S., Kang, Y. and Bae, S. (2022), "Searching for new technology acceptance model under social context: analyzing the determinants of acceptance of intelligent information technology in digital transformation and implications for the requisites of digital sustainability", *Sustainability*, Vol. 14 No. 1, p. 579, doi: 10.3390/su14010579.

Pearson, S. and Charlesworth, A. (2009), *Accountability as a Way Forward for Privacy Protection in the Cloud, Cloud Computing*, Springer, Berlin, Heidelberg.

Pirzada, P., Wilde, A., Doherty, G.H. and Harris-Birtill, D. (2021), "Ethics and acceptance of smart homes for older adults", *Informatics for Health and Social Care*, Vol. 47 No. 1, pp. 10-37, doi: 10.1080/17538157.2021.1923500.

Plotkin, D. (2020), *Data Stewardship : An Actionable Guide to Effective Data Management and Data Governance*, Elsevier Science & Technology, San Diego.

Prakash, A.V. and Das, S. (2022), "Explaining citizens' resistance to use digital contact tracing apps: a mixed-methods study", *International Journal of Information Management*, Vol. 63, 102468, doi: 10.1016/j.ijinfomgt.2021.102468.

Prati, A., Shan, C. and Wang, K.I.-K. (2019), "Sensors, vision and networks: from video surveillance to activity recognition and health monitoring", *Journal of Ambient Intelligence and Smart Environments*, Vol. 11 No. 1, pp. 5-22, doi: 10.3233/AIS-180510.

Princi, E. and Krämer, N.C. (2020), "Out of control – privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices", *Frontiers in Psychology*, Vol. 11, pp. 1-15, doi: 10.3389/fpsyg.2020.582054.

Puntoni, S., Reczek, R.W., Giesler, M. and Botti, S. (2021), "Consumers and artificial intelligence: an experiential perspective", *Journal of Marketing*, Vol. 85 No. 1, pp. 131-151, doi: 10.1177/0022242920953847.

Ram, S. and Sheth, J.N. (1989), "Consumer resistance to innovations: the marketing problem and its solutions", *Journal of Consumer Marketing*, Vol. 6 No. 2, pp. 5-14, doi: 10.1108/EUM0000000002542.

Reychav, I., Beeri, R., Balapour, A., Raban, D.R., Sabherwal, R. and Azuri, J. (2019), "How reliable are self-assessments using mobile technology in healthcare? The effects of technology identity

and self-efficacy", *Computers in Human Behavior*, Vol. 91, pp. 52-61, doi: 10.1016/j.chb.2018.09.024.

Ruotsalainen, P. and Blobel, B. (2022), "Transformed health ecosystems—challenges for security, privacy, and trust", *Frontiers of Medicine*, Vol. 9, pp. 1-10, doi: 10.3389/fmed.2022.827253.

Salehi-Amiri, A., Jabbarzadeh, A., Hajiaghaei-Keshteli, M. and Chaabane, A. (2022), "Utilizing the internet of things (IoT) to address uncertain home health care supply chain network", *Expert Systems with Applications*, Vol. 208, 118239, doi: 10.1016/j.eswa.2022.118239.

Sarstedt, M., Henseler, J. and Ringle, C.M. (2011), "Multigroup analysis in partial least squares (PLS) path modeling: alternative methods and empirical results", in Sarstedt, M., Schwaiger, M. and Taylor, C.R. (Eds), *Measurement and Research Methods in International Marketing*, Emerald Group Publishing, Vol. 22, pp. 195-218, doi: 10.1108/s1474-7979(2011)0000022012.

Schneider, J., Abraham, R., Meske, C. and Vom Brocke, J. (2023), "Artificial intelligence governance for businesses", *Information Systems Management*, Vol. 40 No. 3, pp. 229-249, doi: 10.1080/10580530.2022.2085825.

Shaw, N. and Sergueeva, K. (2019), "The non-monetary benefits of mobile commerce: extending UTAUT2 with perceived value", *International Journal of Information Management*, Vol. 45, pp. 44-55, doi: 10.1016/j.ijinfomgt.2018.10.024.

Shrout, P.E. and Bolger, N. (2002), "Mediation in experimental and nonexperimental studies: new procedures and recommendations", *Psychological Methods*, Vol. 7 No. 4, pp. 422-445, doi: 10.1037/1082-989X.7.4.422.

Sivakumar, C., Mone, V. and Abdumukhtor, R. (2024), "Addressing privacy concerns with wearable health monitoring technology", *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, Vol. 14 No. 3, e1535, doi: 10.1002/widm.1535.

Smith, H.J., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly*, Vol. 35 No. 4, pp. 989-1015, doi: 10.2307/41409970.

Solove, D.J. (2006), "A taxonomy of privacy", *University of Pennsylvania Law Review*, Vol. 154 No. 3, pp. 477-564, doi: 10.2307/40041279.

Someh, I., Davern, M., Breidbach, C.F. and Shanks, G. (2019), "Ethical issues in big data analytics: a stakeholder perspective", *Communications of the Association for Information Systems*, Vol. 44, pp. 718-747, doi: 10.17705/1CAIS.04434.

Son, J.-Y. and Kim, S.S. (2008), "Internet users' information privacy-protective responses: a taxonomy and a nomological model", *MIS Quarterly*, Vol. 32 No. 3, pp. 503-529, doi: 10.2307/25148854.

Stavropoulos, T.G., Papastergiou, A., Mpaltadoros, L., Nikolopoulos, S. and Kompatsiaris, I. (2020), "IoT wearable sensors and devices in elderly care: a literature review", *Sensors*, Vol. 20 No. 10, 2826, doi: 10.3390/s20102826.

Sun, L., Yang, B., Kindt, E. and Chu, J. (2024), "Privacy barriers in health monitoring: scoping review", *JMIR Nursing*, Vol. 7, e53592, doi: 10.2196/53592.

Talal, M., Zaidan, A., Zaidan, B., Albahri, A.S., Alamoodi, A., Albahri, O.S., Alsalem, M., Lim, C.K., Tan, K.L., Shir, W. and Mohammed, K.I. (2019), "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review", *Journal of Medical Systems*, Vol. 43 No. 3, 42, doi: 10.1007/s10916-019-1158-z.

Tallon, P.P. (2013), "Corporate governance of big data: perspectives on value, risk, and cost", *Computer*, Vol. 46 No. 6, pp. 32-38, doi: 10.1109/MC.2013.155.

Talwar, S., Dhir, A., Islam, N., Kaur, P. and Almusharraf, A. (2023), "Resistance of multiple stakeholders to e-health innovations: integration of fundamental insights and guiding research paths", *Journal of Business Research*, Vol. 166, 114135, doi: 10.1016/j.jbusres.2023.114135.

Taylor, S.J., Bogdan, R. and DeVault, M. (2016), *Introduction to Qualitative Research Methods: A Guidebook and Resource*, 4th ed., John Wiley & Sons, Incorporated, Hoboken.

Timan, T. and Albrechtslund, A. (2018), "Surveillance, self and smartphones: tracking practices in the nightlife", *Science and Engineering Ethics*, Vol. 24 No. 3, pp. 853-870, doi: 10.1007/s11948-015-9691-8.

Trampusch, C. (2024), "Regulating the digital economy: explaining heterogenous business preferences in data governance", *Journal of European Public Policy*, Vol. 31 No. 7, pp. 1902-1926, doi: 10.1080/13501763.2023.2181853.

Trkman, M., Popovič, A. and Trkman, P. (2023), "The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications", *Government Information Quarterly*, Vol. 40 No. 1, 101787, doi: 10.1016/j.giq.2022.101787.

van Donge, W., Bharosa, N. and Janssen, M. (2022), "Data-driven government: cross-case comparison of data stewardship in data ecosystems", *Government Information Quarterly*, Vol. 39 No. 2, 101642, doi: 10.1016/j.giq.2021.101642.

Van Zoonen, L. (2016), "Privacy concerns in smart cities", *Government Information Quarterly*, Vol. 33 No. 3, pp. 472-480, doi: 10.1016/j.giq.2016.06.004.

Venkatesh, V., Brown, S.A. and Bala, H. (2013), "Bridging the qualitative-quantitative divide: guidelines for conducting mixed methods research in information systems", *MIS Quarterly*, Vol. 37 No. 1, pp. 21-54, doi: 10.25300/MISQ/2013/37.1.02.

Venkatesh, V., Brown, S.A. and Sullivan, Y.W. (2016), "Guidelines for conducting mixed-methods research: an extension and illustration", *Journal of the Association for Information Systems*, Vol. 17 No. 7, pp. 435-494, doi: 10.17705/1jais.00433.

Vigurs, C., Maidment, C., Fell, M. and Shipworth, D. (2021), "Customer privacy concerns as a barrier to sharing data about energy use in smart local energy systems: a rapid realist review", *Energies*, Vol. 14 No. 5, pp. 1-31, doi: 10.3390/en14051285.

Wang, X., McGill, T.J. and Klobas, J.E. (2020), "I want it anyway: consumer perceptions of smart home devices", *Journal of Computer Information Systems*, Vol. 60 No. 5, pp. 437-447, doi: 10.1080/08874417.2018.1528486.

Wang, H., Mao, K., Wu, W. and Luo, H. (2023), "Fintech inputs, non-performing loans risk reduction and bank performance improvement", *International Review of Financial Analysis*, Vol. 90, 102849, doi: 10.1016/j.irfa.2023.102849.

Weber, R.H. (2010), "Internet of things–new security and privacy challenges", *Computer Law and Security Report*, Vol. 26 No. 1, pp. 23-30, doi: 10.1016/j.clsr.2009.11.008.

Wilson, J., Heinsch, M., Betts, D., Booth, D. and Kay-Lambkin, F. (2021), "Barriers and facilitators to the use of e-health by older adults: a scoping review", *BMC Public Health*, Vol. 21, pp. 1-12, doi: 10.1186/s12889-021-11623-w.

Wu, X., Xiong, J., Yan, J. and Wang, Y. (2021), "Perceived quality of traceability information and its effect on purchase intention towards organic food", *Journal of Marketing Management*, Vol. 37 Nos 13-14, pp. 1267-1286, doi: 10.1080/0267257X.2021.1910328.

Xu, Z. (2019), "An empirical study of patients' privacy concerns for health informatics as a service", *Technological Forecasting and Social Change*, Vol. 143, pp. 297-306, doi: 10.1016/j.techfore.2019.01.018.

Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi, Y. (2022), "Blockchain for healthcare data management: opportunities, challenges, and future recommendations", *Neural Computing and Applications*, Vol. 34 No. 14, pp. 1-16, doi: 10.1007/s00521-020-05519-w.

Zhu, Y., Lu, Y., Gupta, S., Wang, J. and Hu, P. (2022), "Promoting smart wearable devices in the health-AI market: the role of health consciousness and privacy protection", *The Journal of Research in Indian Medicine*, Vol. 17 No. 2, pp. 257-272, doi: 10.1108/JRIM-10-2021-0246.

Zuzul, T.W. (2019), "Matter battles: cognitive representations, boundary objects, and the failure of collaboration in two smart cities", *Academy of Management Journal*, Vol. 62 No. 3, pp. 739-764, doi: 10.5465/amj.2016.0625.

Corresponding author
Jingjing Zhang can be contacted at: jingjing.zhang@autuni.ac.nz