

Binzer, Björn; Kendziorra, Jennifer; Witte, Anne-Katrin; Winkler, Till J.

Article — Published Version

Trust in Public and Private Providers of Health Apps and Usage Intentions

Business & Information Systems Engineering

Suggested Citation: Binzer, Björn; Kendziorra, Jennifer; Witte, Anne-Katrin; Winkler, Till J. (2024) : Trust in Public and Private Providers of Health Apps and Usage Intentions, Business & Information Systems Engineering, ISSN 1867-0202, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 66, Iss. 3, pp. 273-297,
<https://doi.org/10.1007/s12599-024-00869-4>

This Version is available at:

<https://hdl.handle.net/10419/315714>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<http://creativecommons.org/licenses/by/4.0/>



Trust in Public and Private Providers of Health Apps and Usage Intentions

A Sectoral Privacy Calculus and Control Perspective

Björn Binzer · Jennifer Kendziorra · Anne-Katrin Witte · Till J. Winkler

Received: 1 July 2023 / Accepted: 2 April 2024 / Published online: 11 June 2024
© The Author(s) 2024

Abstract Mobile health apps, particularly personal health records (PHRs), play a vital role in healthcare digitalization. However, the varying governance approaches for providing PHR platforms have led to a growing debate on the adequate regulation of health technology with regard to their adoption. This article investigates how provider governance, whether public or private, influences users' intentions to use and decisions to download a PHR app. Drawing on institutional trust, privacy calculus, and privacy control frameworks, the study develops hypotheses about how provider governance affects the pathways through which trust influences users' intentions to adopt the app. Data acquired from an online experiment in the German market reveals that users exhibit a higher level of trust in public providers compared to the same app provided by private companies. Furthermore, provider governance significantly alters the paths in how trust influences usage intentions through perceived benefits, perceived risks, and

privacy control. These findings contribute to the development of a sectoral theory of privacy calculus and privacy control in Information Systems (IS). Moreover, they offer practical insights for healthcare regulators and health app providers with the aim of promoting the acceptance and usage of PHRs and other mobile health apps.

Keywords Mobile health · Digital health · Personal health records · Adoption · Usage intention · Privacy calculus · Privacy control

1 Introduction

Mobile health apps such as personal health records (PHR) are considered crucial for healthcare digitalization as they enable individuals to manage their personal health effectively (Archer et al. 2011; George and Kohnke 2018). PHRs assist users in accessing, integrating, and organizing their personal health information, thereby enhancing communication between patients and healthcare providers (Abd-alrazaq et al. 2019; Niazkhani et al. 2020; Tang et al. 2006). However, national health systems employ varying governance approaches for providing PHR platforms (Lee et al. 2021) and there is a small, but growing debate as to which level of regulation, e.g., for privacy in health information exchange, is adequate to drive health technology adoption (e.g., Adjerid et al. 2016; Miller and Tucker 2009; Tertulino et al. 2023).

Certain countries, such as the Scandinavian countries and France, offer centralized PHR platforms through public health authorities (e.g., Appenzeller 2020; Jensen et al. 2017). Similarly, Germany has enacted legislation requiring its public health insurances to provide and activate PHRs for their insured individuals by 2025, while there is

Björn Binzer and Jennifer Kendziorra have contributed equally to this work.

Accepted after one revision by the editors of the Special Issue.

B. Binzer (✉) · J. Kendziorra (✉) · A.-K. Witte · T. J. Winkler
Faculty of Business Administration and Economics, Chair of
Information Management, University of Hagen, Hagen,
Germany
e-mail: bjoern.binzer@fernuni-hagen.de

J. Kendziorra
e-mail: jennifer.kendziorra@fernuni-hagen.de

T. J. Winkler
e-mail: till.winkler@fernuni-hagen.de

T. J. Winkler
Department of Digitalization, Copenhagen Business School,
Frederiksberg, Denmark

also a growing market of health apps from private providers (Retiene 2022; Schrahe 2021). Other countries with pluralistic healthcare systems, such as the U.S., primarily rely on the private market for the development of health apps. A prominent example is Google that is trying to enter and penetrate the healthcare market with several digital offerings (Jercich 2021), such as the Care Studio platform that offers healthcare professionals an integrated perspective of patient records (Balasubramanian 2022; Google Health 2023). These examples illustrate that PHR adoption contexts vary considerably across countries.

Furthermore, a growing number of competing health apps with similar functionalities is being offered by both public and private providers, even within a single market. For instance, in Germany, the startup XO Life integrates a medication checker into their MedWatcher app for automated testing of drug therapy safety (MedWatcher 2023). This functionality is also part of the roadmap for the ‘elektronische Patientenakte’ (ePA), the PHR provided by public insurance companies in Germany, as outlined in the recent digital strategy of the federal ministry of health (Bundesministerium für Gesundheit 2023). While the provision of the ePA will be mandatory for public insurers by 2025, users have the possibility to opt out of its activation. This legally prescribed provision, but voluntary use of PHR apps on the market raises the legitimate need for app providers and healthcare regulators to better understand how provider governance (i.e., whether public or private) itself affects users’ intentions to use health apps.

Among the many existing mobile health apps, PHRs face particularly complex challenges across most nations (Roehrs et al. 2017). Despite pertinent privacy regulations such as GDPR in Europe, trust in PHR providers remains a major issue, which has hindered the widespread adoption among consumers (Spil and Klein 2015). Researchers from different fields have observed an institutional trust paradox: although public institutions rely on people’s trust to effectively act as their agents (Rothstein and Stolle 2008), consumers in many countries tend to trust private companies and their brands more than their governments (Pesce 2020; Ward et al. 2016). However, it remains to be seen whether this trust paradox extends to the domain of healthcare and the storing of sensitive health data in PHRs.

Previous research has extensively studied the factors that influence the acceptance of information technologies, highlighting the role of privacy-related factors, such as trust (e.g., Carter and Bélanger 2005; Connolly et al. 2023; Lin et al. 2021), privacy concerns (e.g., Dinev and Hart 2005; Ehrari et al. 2020; Malhotra et al. 2004), and privacy control (e.g., Dinev et al. 2016; Li et al. 2014). Trust, privacy control, and perceived benefits have consistently been found to have a positive impact on the intention to use an app, while perceptions of privacy and security risks tend

to decrease it. However, there is a lack of theoretical development regarding the influence of the app providers’ governance on the user’s behavioral intention to use a health app. This presents a major gap in our knowledge, considering that previous research has demonstrated varying levels of trust in different institutions (Ward et al. 2016). Understanding the impact of provider governance on people’s trust perceptions, usage intentions, and decisions to ultimately download and use a health app could be a key to address the persistent trust challenges associated with PHRs in healthcare. Consequently, this study aims to answer the following question: *How does provider governance influence the behavioral intention to use and the decision to download a mobile health app?*

Taking our vantage point in an institutional trust perspective, we first hypothesize that different governance types (*public*: health authority and public insurance; *private*: big company and startup) influence trust in the app provider. Extending the prevalent privacy calculus and privacy control perspectives, we then propose three differential effects by which provider governance may affect the pathways of trust on intentions to use through perceived benefits, perceived risks, and perceived privacy control. To test these hypotheses, we conducted an online experiment in the German market, framing it as a user study of a real PHR app in development. Participants were randomly assigned to one of four provider governance scenarios and asked to evaluate the simulated app.

Contrary to the public/private trust paradox, our results demonstrate that users have higher trust in a public health app provider compared to the same health app provided by a private company, even though public providers are attested to have lower abilities. Furthermore, utilizing partial least squares (PLS) multigroup analysis methods, we find that provider governance significantly alters the pathways through which trust influences intentions to use the app. This is particularly the case with regard to perceived benefits, perceived risks, and perceived control. Usage intentions, in turn, significantly predict the decision to download the app. Our findings suggest that private health app providers, despite generally enjoying lower levels of trust, can influence usage intentions and downloads more strongly by leveraging benefit perceptions and privacy controls compared to public providers. Contrary to our hypothesis, public providers can influence the intention to use and download decision to a higher degree than private ones by mitigating the perceived risks.

Our study contributes a sectoral theory of privacy calculus and privacy control to research in Information Systems (IS) by accounting for the different forms of governance among trusted institutions. In addition, our results also call into question the widespread conceptualization of ability as a trust component. On a practical level,

our findings offer insights for health app providers and healthcare regulators to enhance the adoption and usage of PHRs and other health apps. In the following sections, we develop the research hypotheses, describe the methods employed, present the results, and discuss the theoretical and practical implications.

2 Related Work and Hypothesis Development

This section takes its vantage point in the institutional trust perspective whereby we hypothesize the influence of provider governance on trust in health app providers. We then introduce the privacy calculus (i.e., perceived benefits and perceived risks) and perceived control to explain how trust translates into usage intentions, and develop our hypotheses of how provider governance alters these pathways in the context of PHR apps.

2.1 An Institutional Perspective on Trust in the Provider

The construct of trust has motivated many scholars from various disciplines such as psychology, marketing, and IS to explore its various aspects and peculiarities (Ebert 2009). A multitude of conceptualizations, measures, and antecedents of trust have emerged in the literature (Söllner and Leimeister 2013). In this study, we follow an adapted version of the widely cited definition proposed by Mayer et al. (1995) and define trust as *the willingness of a trustor to be vulnerable to the actions of a trustee based on the expectation that the trustee will perform a particular action relevant and important to the trustor, irrespective of the ability to monitor the respective trustee* (Söllner and Leimeister 2013). A trustee's specific characteristics are of great relevance in this relationship, as the trustors' willingness to trust is based on their assessment of these characteristics (Söllner et al. 2016a).

Previous research conceptualized three important components of trusting beliefs: a trustee's ability, benevolence, and integrity (Mayer et al. 1995). *Ability* reflects the trustor's perception that the trustee's competencies, skills, and task-related activities demonstrate expertise and enable the trustee to succeed in a specific domain (Mayer et al. 1995; Söllner 2020). *Benevolence* reflects the trustor's perception that the trustee demonstrates an overall positive orientation towards the trustor and wants to do good to the trustor (Mayer et al. 1995; Söllner 2020). *Integrity* reflects the trustor's perception that the trustee adheres to a set of principles, values, and ideals that are acceptable to the trustor (Mayer et al. 1995; Söllner 2020). This study considers these components as separate constructs in addition to overall trust in the provider.

While prior research has identified multiple trust relationships and trust targets that are relevant for IS research (Söllner et al. 2016b), this study specifically examines trust in the provider of a mobile health app. In this context, the app user assumes the role of the trustor, while the app provider constitutes as the trustee. The importance of users' trust in the provider of an information technology for the acceptance has been demonstrated by numerous studies (e.g., Mittendorf 2017; Robin and Dandis 2021; Söllner 2020). However, most of the existing research has focused on a single provider and thus neglected possible differences in the individuals' perceptions of different provider types.

Only a limited number of studies have placed emphasis on potential differences between providers. For instance, in an e-commerce context, Jarvenpaa et al. (2000) tested in an experiment how trust perceptions differ between online store types (e.g., online bookstores and online travel sites) and found significant differences. Bansal et al. (2016) used a controlled lab experiment in which they presented users with website stimuli from contexts with different monetary sensitivity (i.e., financial, health, and e-commerce websites) and concluded that context is a salient factor for trust formation which is critical for disclosing personal information online. In a healthcare context, Anderson and Agarwal (2011) explored an individual's trust and decision to disclose personal health information to different stakeholders. The study found significant differences in the willingness to disclose information to hospitals compared to governmental agencies, but not between pharmaceutical companies and governmental agencies.

Given the growing debate on the healthcare technology regulation, this study focuses on the governance between public and private forms as an essential provider characteristic. Specifically, we consider two possible types of public providers of healthcare apps that play a key role in different healthcare system contexts: health authorities and public insurances. *Health authorities* are governmental bodies responsible for health policy-making which provide oversight of the health sector. By definition, health authorities are public institutions whose operations are financed by tax revenues. Countries like Denmark and France exemplify the provision of PHR infrastructures by health authorities (Appenzeller 2020; Jensen et al. 2017). On the other hand, *public insurances* are, in the context of this study, classified as corporations under public law that play a vital role in fulfilling public interest tasks such as healthcare service reimbursement. Thus, they are highly regulated, but legally independent entities. In Germany, for instance, there are currently 96 statutory (i.e., public) health insurances covering approximately 90% of the population (GKV Spitzenverband 2023).

In addition, our study considers two types of private providers of PHR apps that represent opposite ends of the

maturity spectrum: big companies and startups. *Big companies* are conceptualized as large corporations and characterized by their well-established brands and diversified operations, which may include involvement in the health-care market. These companies are subject to corporate laws and are held accountable not only financially, but also in terms of social responsibility. Examples of big companies in Germany providing health apps (amongst other services) include firms like Siemens and SAP SE. *Startup companies* are smaller firms focusing on developing innovative mobile health solutions, such as PHR apps. Notable cities like Boston and Berlin boast dynamic startup ecosystems fervently engaged in the burgeoning digital health market (Judah et al. 2020). Both, big companies and startups, are keenly involved in the mobile health sector. For instance, the global software market for PHRs is projected to surpass 15 billion US dollars by 2030 (Zion Market Research 2023). Table 1 presents an overview of the key attributes of these four provider types.

Because a trustee's characteristics are relevant for the trustors' willingness to trust, we propose that the level of trust depends on the distinction between public and private health app providers. A recent survey on mobile apps for pandemic research differentiated between governmental and private organizations, revealing that this distinction was significant for the level of trust that users placed in the apps (Buhr et al. 2022). Public institutions, by definition, have the mandate to serve and take care of the population (Rothstein and Stolle 2008), with healthcare being a part of their responsibilities in most countries. Hence, there is a high degree of coherence between the mission of public institutions to serve the public good (Rainey et al. 2021) and the task to preserve the highly sensitive health data. Their high degree of accountability to the public makes health authorities a generally trusted provider of health technologies, including PHR apps. Private institutions such as companies, in contrast, have inherently different objectives. While many companies consider social responsibility as a part of their mission, their primary focus is on generating profits. This raises concerns that private providers may prioritize profit opportunities over users' privacy

(Anderson and Agarwal 2011). For instance, a study related to fears of health data sharing revealed that two of four concerns were explicitly associated with potential data exploitation by private companies (Lounsbury et al. 2021). Therefore, we hypothesize:



Hypothesis 1 Trust and its components (ability, benevolence, integrity) will be higher for public providers of health apps and lower for private providers.

2.2 Provider Governance Altering the Trust-Usage Intention Pathways

Prior IS research has consistently demonstrated a relationship between trust and usage intentions. For example, trust influences the intended use of a B2C website in ecommerce (Gefen and Straub 2003) and the intentions to use an e-government system (Carter and Bélanger 2005). In the following, we draw on privacy calculus and privacy control perspectives to explicate the different pathways that explain the trust-usage relationship. Linking back to our provider governance conceptualization, we then develop three hypotheses of how provider governance alters these pathways. Figure 1 displays our research model and hypotheses.

Considering that the storing of sensitive health data in mobile apps may exacerbate people's concerns about potential misuse of their health data, the intention to use a health app involves a privacy calculus (Li et al. 2014). The privacy calculus is a widely accepted model which posits that individuals make privacy decisions based on a process of weighing the anticipated benefits and risks of this decision (Culnan and Bies 2003; Laufer and Wolfe 1977). This implies that individuals, when confronted with the choice of using a health app that necessitates the disclosure of personal information, evaluate the anticipated benefits and potential risks associated with the technology, which ultimately impacts their decision-making process regarding adoption. In this context, it is important to acknowledge the complex interplay between perceived risks, benefits, and the often opaque nature of data usage. Consequently, it is

Table 1 Provider governance and provider type conceptualization

Governance	Public governance 		Private governance 	
	Health authority	Public insurance	Big company	Startup company
Ownership	Public institution	Public law company	Publicly listed company	Private company
Regulation	Regulator	Highly regulated	Considerably regulated	Moderately regulated
Economy	Tax financed	Membership financed	Profit-based	Venture funding
Competence	Policy & oversight	Reimbursement	Services at scale	Innovation

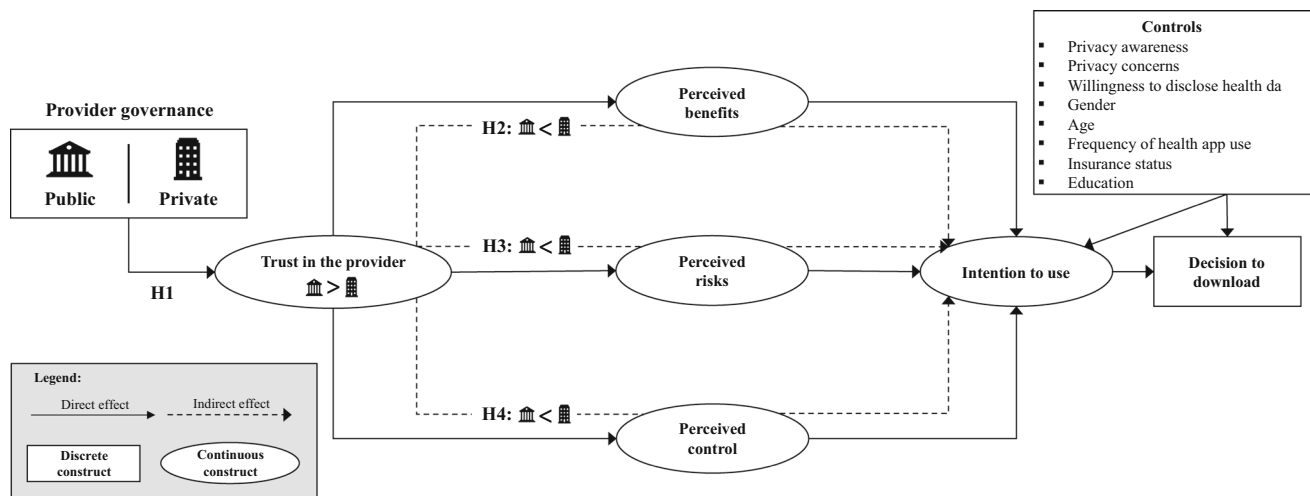


Fig. 1 Research model

crucial to consider the incomplete information users often have about how their data been used (often perceived as ‘black box’) and the behavioral biases that may influence their decision-making.

Furthermore, when researching privacy decisions, it is essential to consider the context (Acquisti et al. 2015; Yun et al. 2019). Smith et al. (2011) identified four contextual forces related to privacy beliefs: the type of collected information, the use of information by sector, the technological applications, and the political context. In the context of our study, we refer to personal health data such as vital parameters, diagnoses, test results, and medication plans. This data can be used to enhance care processes, improve clinical outcomes, and drive advancement of research within the healthcare sector. The technological application is a PHR, a digital platform that enables individuals to access, manage, and share their personal health information with healthcare professionals within a private, secure, and confidential environment (Tang et al. 2006). The political context of our study is Germany, a country with high privacy sensitivity (Bellman et al. 2004) that has not yet achieved widespread adoption of any PHR platform (Schrahe 2021). In the following, we conceptualize the perceived benefits and perceived risks of PHRs for the context of this study and elaborate on perceived control.

2.2.1 Perceived Benefits Pathway and Provider Governance

As patients often receive care from many different healthcare providers, their health data are commonly dispersed over various facilities and stored in different analog and digital formats. In general, PHRs are seen as a major development towards the digitization of healthcare systems, with the purpose of improving quality and lowering

the costs of healthcare (Bandyopadhyay et al. 2012), leading to various types of benefits a PHR app may provide to its users. The extent of perceived benefits of an app positively influences users’ intentions to download it (Eling et al. 2013; Harris et al. 2016) and also affects their willingness to share personal information with the app (Wotrich et al. 2018). Prior works have emphasized different benefits of PHRs.

For example, PHRs enable timely and location-independent access to a wide array of personal health information (Tang et al. 2006). Such health information can stem from different systems used by caregivers and health professionals authorized by the patient (Tang et al. 2006). Access to their information helps patients to manage their health and monitor diseases more effectively in conjunction with their healthcare providers. In addition, PHRs can strengthen the health literacy of patients by providing them with knowledge about their own care. This results in patients’ enhanced ability for more effective healthcare management. PHRs give patients control over their health records and data and empower them to become active participants in their own care (Tang et al. 2006). Furthermore, PHRs can improve healthcare quality due to earlier identification of adverse events, defined as injuries that are caused by medical management, such as medication errors (Bandyopadhyay et al. 2012) and avoidance of duplicate examinations. Involving patients in their own care through a PHR can promote prevention and more timely interventions and thus disburden the healthcare system. Lastly, PHRs can enhance the communication between patients and physicians when they are collaboratively tracking the patient’s health. This can help overcome information asymmetries and reduce communication barriers. PHRs may even change physician encounters from episodic to

continuous, which should make it easier for the patients to ask questions (Tang et al. 2006).

Despite the common features of a PHR, each individual will evaluate these benefits depending on the respective context (Smith et al. 2011). Trust in the provider influences an individual's perception of an information system offered by that provider, including its perceived usefulness and benefits (Söllner et al. 2016b). The influence of trust on perceived benefits has been substantiated in other contexts such as e-commerce (Kim et al. 2009) and e-services (Mou and Cohen 2014). Furthermore, in line with previous research (e.g., Gong et al. 2019; Li et al. 2014), perceived benefits likely increase an individual's usage intention for a PHR app. For example, Gong et al. (2019) highlighted the importance of perceived benefits on the intentions to use an online health consultation service; Li et al. (2014) found a strongly positive effect of benefits on the intention to use a standalone PHR app. Against this background, we expect to find a pathway in which *trust positively influences the perceived benefits of a mobile health app and perceived benefits, in turn, positively influence the intention to use*.

What is unknown, however, is whether the characteristics of the organization handling personal health information, specifically the provider's governance, will influence this pathway. Such influence could arise from the distinct economic and competence-related characteristics that differentiate these institutions (see Table 1). Private companies, driven by market-differentiation, may have a greater incentive to promote their products (e.g., mobile PHRs) even if these do not yet fully satisfy the benefit expectations, leading to user suspicion. Therefore, users that do not trust a private provider, will not expect the promised benefits to materialize. Low perceived benefits, in turn, will be associated with low usage intentions. Users who *do* trust a private provider, however, will likely have great benefit expectations and also higher usage intentions due to the private provider's presumed competency in providing innovative services at scale. Higher benefits expectations from the privately provided app should also translate into high usage intentions, as users will anticipate that this market offering will effectively meet their specific needs. It is, therefore, a necessary requirement that users trust the private provider and its offering, before making a positive benefit evaluation and forming their usage intentions.

Innovation and economic incentives are less pronounced in the public sector (Arundel et al. 2019) and public providers are generally seen as having less competence in providing effective solutions than the private sector (Hvidman 2019). Consequently, users might rather expect a 'standard' service from a public provider of a health app regardless of their trust in this public institution. In other words, there is likely less variation in the perceived benefits depending on trust in public providers compared to

private providers. Conversely, users' intention to use a publicly provided app may be less influenced by expectations of benefits. This is because public health apps might be viewed more as a societal obligation or a common good rather than a personal consumer choice (Galetsi et al. 2023). Hence, for publicly provided apps, the usage intentions might be less rooted in benefits expectations than for private providers' apps. In summary, we suggest that both, the effect of trust in the provider on perceived benefits and the effect of perceived benefits on intention to use differ between public and private providers. Therefore, we pose:

Hypothesis 2 The positive indirect effect of trust on intention to use via perceived benefits will be stronger for private providers and weaker for public providers.

2.2.2 Perceived Risks Pathway and Provider Governance

The second component of the privacy calculus is the perception of risks associated with a privacy-related decision. Perceived risks can be defined as "*the subjective belief that there is some probability of suffering a loss in pursuit of a desired outcome*" (Pavlou and Gefen 2004). Uncertainty about possible consequences can negatively impact the net outcome of the privacy calculus and, consequently, the intention to use (Featherman and Pavlou 2003; Flavián and Guinalú 2006). Depending on the context, certain types of risks can be more important than others. The healthcare domain is characterized by highly sensitive information and a plurality of stakeholders, thus leading to a broad range of risks that need to be considered (Anderson and Agarwal 2011). Moreover, in light of potential hazards such as data abuse or misuse, particularly concerning sensitive health information, and considering the diverse and perhaps unexpected uses of this data, it's crucial to address the 'black box' nature of PHR apps. Individuals often possess limited information regarding organizational practices or the implications of their data sharing. This gap in understanding can lead to an unawareness of the true value and potential consequences of sharing personal information (Deuker 2010). Such lack of awareness hampers individuals' ability to accurately assess risks, thus influencing their decision-making and benefit realization.

Trust has been identified as a significant antecedent of perceived risks (Culnan and Armstrong 1999). When trust in a provider is high, the subjective risks associated with using the system seem lower from a user perspective (e.g., Kim et al. 2009; Mou and Cohen 2014). Perceived risks, in turn, negatively influence the behavioral intentions to use information systems (e.g., Li et al. 2014; Nicolaou and McKnight 2006). For instance, Li et al. (2014) showed that lower perceived risks of a standalone PHR, such as

Microsoft HealthVault, increase the users' intentions to use this system. Perceived risks form the second part of the equation of the privacy calculus. Taken together, we expect to find a second pathway in which *trust influences the perceived risks of a mobile health app, and perceived risks, in turn, influence intention to use*.

Open for investigation is the potential role that provider governance may play for this pathway. The influence of trust on perceived risk might differ between public and private providers due to the economic and regulatory characteristics that distinguish these institutions (see Table 1). Users may feel that profit-driven companies have an incentive to exploit their users' health data (Anderson and Agarwal 2011), especially considering potential regulatory loopholes (Lounsbury et al. 2021). Therefore, trust in the provider is likely a necessary requirement to mitigate risk perceptions with private providers. Furthermore, risk perceptions with private providers can also be expected to play a major role for usage intentions. Due to the black box nature of PHR apps and the lingering fears of potential data exploitation by private companies (Lounsbury et al. 2021), perceived risks are likely to have a great impact on usage intentions. The failure of Google Health, for example, was largely attributed to Google's inability to build trust with consumers (O'Mara 2015).

Public providers, in contrast, are subject to strict regulations and do not operate for profit (Rainey et al. 2021). As a result, whether users trust a public institution or not may have a lower impact on perceived risks, as users may have confidence that regulations will prevent the misuse of their data. Placing high trust in a public institution will have lesser impact on perceived risks, too, because users might not assume negative intentions of that institution in the first place (Buhr et al. 2022). In a similar vein, the strong regulatory oversight and accountability of public providers should generally instill more confidence in data safety and ethical handling. This is likely to lead to less emphasis on perceived risks in individuals' decision-making on potential adoption. In sum, we argue that the nature of the provider impacts how perceived risks influence user intentions. We hypothesize:

Hypothesis 3 The positive indirect effect of trust on intention to use via perceived risks will be stronger for private providers and weaker for public providers.

2.2.3 Perceived Control Pathway and Provider Governance

A construct frequently mentioned in conjunction with the privacy calculus is perceived (privacy) control. Perceived control refers to "*the individual's perception of being able to control access to and use of their information*" (Bartol

et al. 2022). While the actual control allows people to choose what and how much data to reveal, it is often the perceived level of control which determines the (disclosure) behavior (Princi and Krämer 2020). In prior studies, researchers have found a control paradox. People who feel in control of their personal data tend to reveal more information even though the objective risks may increase. Conversely, people who perceive a lower level of control may disclose less information, even though the actual risks associated with disclosure may be lower (Brandimarte et al. 2013).

Privacy control has been extensively studied in relation to various factors, including perceived risks, privacy concerns, and trust. Especially the relationship between trust and perceived control has been explored from different perspectives and in diverse contexts (e.g., Dinev et al. 2016; Fox et al. 2022; Li et al. 2014; Saengchai et al. 2020). While trust and perceived control can be considered as two factors in the same nomological layer influencing privacy concerns (Dinev et al. 2016) and intention to use (Li et al. 2014), they might also influence each other. For instance, Fox et al. (2022) investigated how perceived control influences the perceived trustworthiness in online interactions. Saengchai et al. (2020) examined the mediating role of perceived control in the relationship between citizen trust and the adoption of e-government services. Moreover, Robin and Dandis (2021) found that a lack of trust can be offset by the presence of perceived control.

In the context of this study on a PHR app, we adopt the perspective that provider trust is an antecedent of perceived control rather than an outcome. We assume that individuals already possess a certain level of trust in the provider organization, which subsequently influences their perception of their ability to control their privacy through the PHR app. In our experiment, participants were initially introduced to the provider organization, allowing their trusting beliefs to form, before testing the prototype app and its privacy controls (see Methodology in Sect. 3). Therefore, we expect to find a third pathway wherein *trust positively influences the perceived control of a mobile health app, and perceived control, in turn, influences intention to use*.

We venture into unexplored theoretical territory by hypothesizing an effect of provider governance on this pathway. There are compelling reasons to believe that the influence of trust on perceived control differs between public and private providers, stemming from the distinctive regulatory and competence-related characteristics that set these institutions apart (see Table 1). Since individuals may associate private organizations with the development of better solutions, those who possess high trust in private providers are more likely to believe that these companies

act in the best interest of users and thus know how to provide superior privacy controls. Conversely, individuals with low trust are likely to perceive a dearth of robust privacy controls due to the lack of relevant regulations that compel private providers to provide a minimum standard of adequate controls. These differences in perceived controls are likely to translate into greater variance in the intentions to use market-provided PHR app. When private providers are perceived to offer advanced data handling features that enhance the users' control over their own privacy (Walker 2016), then consumers will be more willing to adopt their solutions. Private providers that do not offer these controls, however, are unlikely to find and grow their user base.

In contrast, due to the regulated environment, trust in public providers might be a less of a decisive criterion for users to base their perceptions of privacy controls and usage intentions in. Individuals who have low trust in public institutions can assume that a minimum level of privacy controls will be ensured due to the regulated environment. Users who do trust public institutions may likewise expect privacy controls that meet standard requirements rather than superior features, due to lower perceived competence of public providers in providing advanced privacy features (Hvidman 2019). In addition, since public providers are generally perceived as offering more secure and standardized privacy practices by default (Dinev et al. 2008), users are also less likely to base their usage intentions in the perceived controls for public providers than for private providers. In sum, we suggest that provider governance influences the effect of trust on the perceived control and the effect of perceived control on the intentions to use of a mobile health app. We pose:

Hypothesis 4 The positive indirect effect of trust on intention to use via perceived control will be stronger for private providers and weaker for public providers.

2.2.4 Intention to use and Actual Behavior

Understanding the connection between human intentions and actions is no simple undertaking. While a comprehensive approach to technology adoption research should go beyond mere usage intentions, directly measuring actual adoption or usage of a (hypothetical) technology is often difficult in practice. As a result, the intention to use a technology is commonly employed as a more quantifiable proxy for future usage (Venkatesh et al. 2003). This approach is underpinned by the belief that the intention to use a technology effectively forecasts actual usage (Davis et al. 1989) because it reflects an individual's motivational factors and readiness to perform a specific action (Ajzen 1985; Fishbein and Ajzen 1975).

However, it is crucial to acknowledge the recognized intention-behavior gap in this context (Ajzen 1991; Wu and Du 2012). This gap highlights the phenomenon where individuals do not always act on their stated intentions, meaning that intention can be a precursor but does not invariably lead to behavior in form of corresponding actions (Webb and Sheeran 2006). Therefore, technology adoption might be more accurately viewed as a process (Parmar et al. 2022), where the intention to download an app is an essential indicator of potential behavior, but the progression from these intentions to actual behavior involves various factors and is not as straightforward as it might seem.

Despite this gap, research still underscores the crucial importance of intentions as key psychological predictors of behavior (Sheeran 2002), signifying their primary role in forecasting actions. Building on this with established technology acceptance frameworks (Ajzen 1991; Davis et al. 1989), numerous studies have shown that an individual's intentions are significant and reliable indicators of their actual behavior (Pavlou 2003; Shin 2009). This underscores the notion that initial actions, such as downloading an app, are driven by the user's intention to utilize its features and functions (Gokgoz et al. 2021). In alignment with this body of research, we anticipate that *the intention to use a mobile health app influences the decision to download it*.

Table 2 summarizes the core model variables of this research. As control variables, we consider a number of general traits that can influence an individual's behavioral intention to use a mobile health app: First, privacy awareness is included as individuals who possess a high level of awareness of existing privacy regulations and issues may have lower usage intentions due to their personal disposition to value privacy (Xu et al. 2008). Second, privacy concerns are commonly considered as a variable influencing behavioral intentions (Smith et al. 2011). In line with prior research, all four dimensions of privacy concerns are considered, including collection, errors, unauthorized access, and secondary use (Angst and Agarwal 2009; Smith et al. 1996). Third, the general willingness to disclose personal health data is included as it has frequently been investigated as a dependent variable in privacy research that is closely related to usage intentions (Entreß-Fürsteneck et al. 2019). In addition, we consider as control variables a set of socio-demographic characteristics of the users, specifically, gender, age, level of education, frequency of health app use, and insurance status.

Table 2 Research constructs and definitions

Construct	Definition	Guiding references	Operationalization
Provider governance	Legal and economic nature of an institution developing and operating a mobile health app	Ploner et al. (2019)	Two public versus two private provider organization types
Intention to use	Behavioral intention to use a PHR app	Davis et al. (1989); Venkatesh et al. (2003)	Adapted from Venkatesh et al. (2003) & self-developed
Trust in the provider	Trusting beliefs in a particular provider of a health app and its attributes that are favorable for the trustor	Mayer et al. (1995); Söllner and Leimeister (2013); Söllner (2020)	Adapted from Gefen and Straub (2003); Malhotra et al. (2004); McKnight et al. (2002)
Perceived benefits	Belief that the expected outcome of using the outlined PHR app is beneficial and valuable	Li et al. (2014); Mou and Cohen (2014); Tang et al. (2006)	Adapted from Li et al. (2014); Tang et al. (2006) & self-developed
Perceived risks	Belief that the expected outcome of using the PHR app is risky and bears loss potential	Flavián and Guinalíu (2006); Li et al. (2014); Mou and Cohen (2014); Pavlou and Gefen (2004)	Adapted from Dinev and Hart (2006); Flavián and Guinalíu (2006); Li et al. (2014)
Perceived control	Individual's perception of being able to control access to and use of their information	Bartol et al. (2022); Princi and Krämer (2020)	Bartol et al. (2022); Xu et al. (2008)
Download decision	The decision for or against downloading the PHR app	Gokgoz et al. (2021); Pentina et al. (2016)	Observation of download decision (via fictitious app store buttons)

3 Methodology

To address our research objective of investigating the impact of provider governance on the behavioral intention to use a mobile health app, we employed a combination of experimental research and survey methods, thereby responding to calls for greater utilization of the online experiment paradigm in IS research (Fink 2022). In the experimental phase, we developed an interactive click-prototype of a PHR app called ‘*MeineGesundheitsAkte*’ (i.e., English: ‘*MyHealthRecord*’), drawing inspiration from a range of existing PHR apps available in the German market. The front-end design and features of the app were created based on these reference apps. Subsequently, by relying on this template app, we created four variants, differing only in the displayed logo and data processor declarations (name and address) in the privacy statement. Thus, each variant represented a distinct type of app provider.

For reasons of external validity, we selected four providers that (could) realistically provide a PHR app in the German market. To represent the health authority provider type, we chose the *German Bundesministerium für Gesundheit* (Federal Ministry of Health). This choice aligns with the Ministry's majority ownership of Gematik, the operator responsible for the nationwide health information infrastructure in the German healthcare system (Gematik 2022). For the public insurance provider, we selected *Techniker Krankenkasse*, one of the largest statutory health insurances in Germany in terms of members (Statista 2024). As a representative example of a big company with operations in the healthcare sector, we chose

Siemens Healthineers, a medical device company with headquarters in Erlangen, Germany. As a subsidiary of Siemens corporation, Siemens Healthineers has a strong presence in the German market and gained further recognition when it went public in 2021. To represent the startup provider type, we created a fictitious example of a company named *digitalhealth labs* with its distinct name, logo, and company background. Startups are typically characterized as small and relatively unknown companies. By adopting this approach, we were able to maintain control over the specific characteristics and attributes of the startup provider in our study. Figure 2 showcases four variations of the simulated app, displaying selected screens from a total of 20 different screens.

3.1 Operationalization and Experimental Design

Next, we created a survey to measure our research constructs. The items for the constructs of our research model were taken from existing literature (see Table 2), adapted to our context whenever necessary, and translated into German. All constructs were measured using a 5-point Likert scales ranging from ‘I don't agree’ to ‘I agree’ (see Table A1 in online Appendix A; available online via <http://link.springer.com>). All factors employed reflective measurement models.

For *intention to use*, we adapted three items from Venkatesh et al. (2003) to the PHR context and added one self-constructed item (“Once the app is available in the app store, I intend to use *MyHealthRecord*”). *Trust in the provider* was operationalized through seven items adapted from Malhotra et al. (2004) (e.g., “I believe that *Provider*

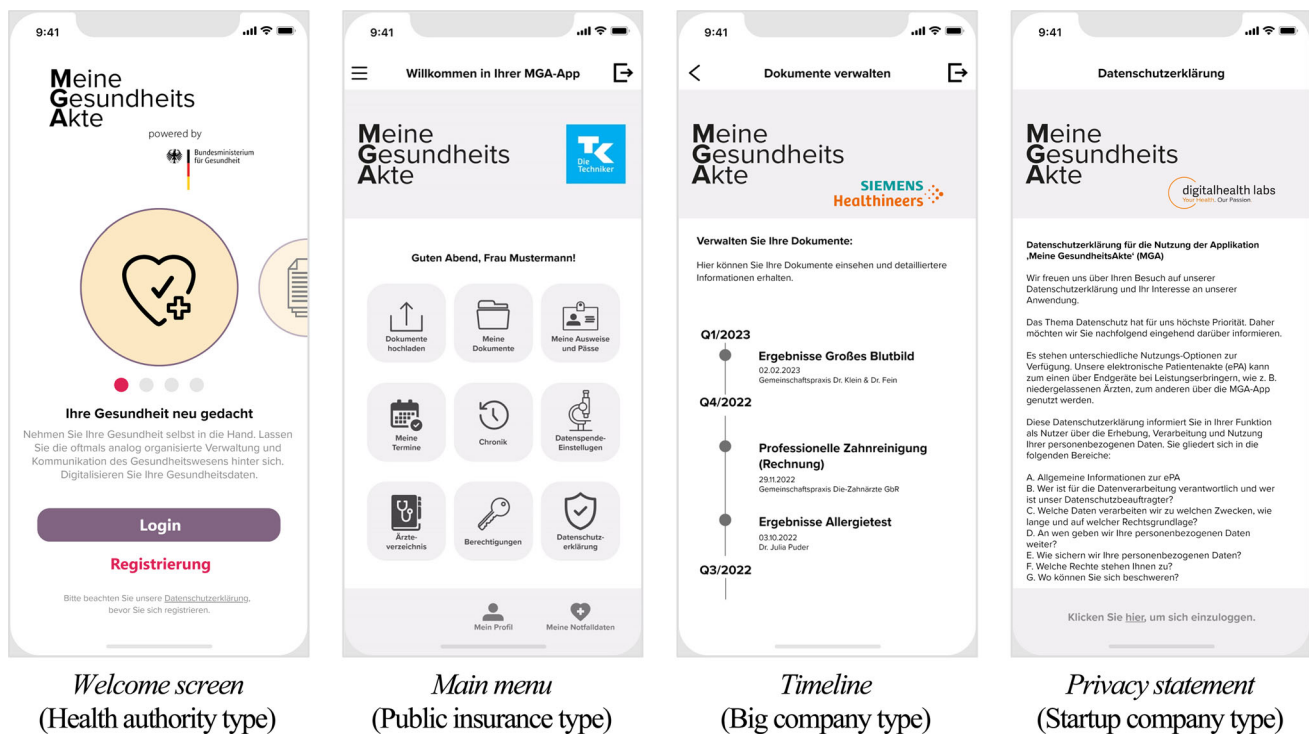


Fig. 2 Example screenshots of the simulated PHR app

is trustworthy”, with *Provider* being replaced by one of the four provider names).

We also measured the ability, benevolence, and integrity components of trust needed for hypothesis 1. *Ability* was measured by adjusting the four items from McKnight et al. (2002) to our study context (e.g., “Overall, *Provider* is a capable and proficient provider of *MyHealthRecord*”). Similarly, we adapted three items for *benevolence* (e.g., “I believe that *Provider* would act in my best interest”) and four items for *integrity* (e.g., “I would characterize *Provider* as honest”) from McKnight et al. (2002). Furthermore, we included one self-developed item for benevolence to enhance the measurement.

To measure *perceived benefits*, we developed four items appropriate for our research context (e.g., “Overall, using *MyHealthRecord* would have a positive impact on my life”). *Perceived risks* were assessed through four adapted items from Li et al. (2014) (e.g., “Overall, the use of *MyHealthRecord* would be risky”). *Perceived control* was measured using the four items proposed by Xu et al. (2008) (e.g., “I believe I have control over who can access my personal health information stored in *MyHealthRecord*”).

Regarding the control variables, *privacy awareness* was measured by four items based on Xu et al. (2008). *Privacy concerns* were assessed by four constructs using slightly adapted items from Angst and Agarwal (2009) about collection, errors, unauthorized access, and secondary use. *Willingness to disclose personal health data* was measured

by using three items based on Entreß-Fürsteneck et al. (2019). In addition, participants were asked to report their *gender* (female, male, diverse/undisclosed), *age* (in years), *frequency of health app use* (on a 6-point scale from daily to never), *education level* (i.e., their highest type of degree), and *insurance status* (whether statutory or private) as additional control variables.

We pre-tested our experiment in think-aloud meetings with nine participants, incorporated the feedback and correspondingly fine-tuned our research design. In the final experiment, participants were presented with a short pre-introduction to the study background and were told that they would participate in a user study of a new health records app that is under development. Participants were not informed in advance about the actual objective of our study in order to avoid biases regarding their attitudes towards the app. Study participants were then randomly assigned to one of the four provider type scenarios. Subsequently, an introduction explaining the PHR app in more detail was shown, which included more background information about the respective provider (e.g., headquarter location and number of employees). After reading the introduction, participants were presented with an interactive simulated app and were tasked to familiarize themselves with the app’s functionalities by clicking through. Participants had to confirm they had understood the app functions before they could proceed.

The survey asked about the participants' intentions to use and to download the app (yes/no) directly after interacting with the app, in order to minimize any bias through privacy-related questions. To capture the *download decision*, we integrated fictitious buttons that claimed to redirect the users to the respective app store upon survey completion. Participants then had to pass through the survey by rating the aforementioned construct items. To ensure that participants understood what they are supposed to evaluate, we included screenshots of the app on each page of the survey. Additional questions about demography, frequency of health-related app usage, and health insurance membership were presented at the end of the survey. On the last page, we debriefed the participants about the true purpose of the study and offered all participants to let us know if, with this additional knowledge, they wanted their answers to be erased (no participant made use of this option).

3.2 Data Acquisition and Sample Description

The data for this study was collected by recruiting anonymous German participants through Prolific, an online data collection platform known for its good data quality (Peer et al. 2021). The data collection period spanned from April 2022 to April 2023. Participants were eligible to participate if they met the pre-screening criteria, which included being a resident of Germany and having German as their first language. To ensure gender balance, we stipulated that the panel should be equally divided between females and males. Participants who successfully completed the approximately 20-min long survey received a small monetary compensation as token of appreciation for their time and effort.

In total, 314 participants completed the online experiment. To ensure the quality of our data, we included one manipulation check and one concentration check question. The 27 participants that failed the manipulation check (i.e., participants were tasked to classify the presented app by one of the four provider types) and the 1 participant that did not pass the concentration check (i.e., "Please indicate that you are still concentrated by selecting 'I agree'.") were removed from the sample, leaving us with a final dataset of 286 participants. With this sample size, a significance threshold of $\alpha = 0.05$ and power of 0.80, sensitivity analyses indicate that *t*-tests detect effect sizes of $d > 0.22$ and the ANOVA employed for subgroup differences detects effects of $f > 0.20$ (Soper 2024). From the full sample of 286, 151 participants completed a questionnaire on a public provider and 135 participants completed a questionnaire on a private provider.

In terms of demographics, the average age of the participants was 31.4 years, and the gender ratio was almost equal (48.3% women and 50.3% men). Participants

reported varying levels of education, and the frequency of using health-related apps was rather low. Most participants reported having public health insurance (90.6%), while 9.4% reported holding a private health insurance. A detailed overview of the demographics of the sample is provided in online Appendix B, Table B1.

3.3 Measurement Model Assessment

We followed the construct validation procedures by MacKenzie et al. (2011) and assessed measurement model validity for our core model (see Fig. 1). Given our focus on testing the differences in trust under Hypothesis 1, we also scrutinized the factor structure for its ability, benevolence, and integrity components. In a first step, we conducted an exploratory factor analysis (EFA) for all core model variables, which confirmed the expected factor structure (see online Appendix C, Table C1). An additional EFA conducted on all trust-related items revealed that the items of *benevolence*, *integrity*, and *trust in the provider* loaded on the same factor. This can be explained by benevolence and integrity being components of trust itself. However, the items of *ability* loaded on a separate factor. When the number of factors is set to four, the highest factor loadings corresponded with the four different constructs (see online Appendix I, Tables I1 and I2).

As a next step, we assessed our measurement model. We employed the consistent PLS algorithm (PLSc), which corrects for inconsistencies in the estimates for reflective factor models (Henseler et al. 2015). Through the assessment of convergent and divergent validity criteria, we identified the need to remove the secondary use dimension from the control variable privacy concerns, two items from dimension error, one item from dimension collection, and one item from dimension unauthorized access (see online Appendix E, Fig. E1). Items of the core model constructs were not concerned. The resulting model constructs demonstrate satisfactory convergent validity based on the quality criteria recommended by Hair et al. (2019). All constructs surpass the recommended thresholds (Hair et al. 2019), with Alpha values above 0.7, composite reliability above 0.7, and average variance extracted above 0.5, see Table 3. This indicates the robustness of the constructs employed in this research and suggests that all items are sufficiently related to their respective constructs. Despite the *privacy awareness-control* variable's resulting AVE value (0.495) being slightly below the recommended threshold, we decided to retain it as a control variable since all other quality criteria were fulfilled.

We assessed the discriminant validity for our core model by the Fornell-Larcker criterion and the heterotrait-mono-trait (HTMT) ratio of correlations (see online Appendix D, Table D1) and by the CICFA technique proposed by

Table 3 Internal consistency and convergent validity criteria

Construct	Cronbach's alpha	Composite reliability	AVE
Intention to use	0.958	0.958	0.852
Trust in the provider	0.957	0.957	0.760
Perceived benefits	0.902	0.903	0.701
Perceived risks	0.912	0.914	0.729
Perceived control	0.899	0.899	0.690
Privacy awareness	0.814	0.784	0.495
PC collection	0.865	0.864	0.682
PC error	0.889	0.890	0.802
PC unauthorized access	0.792	0.792	0.656
Willingness to disclose	0.931	0.931	0.819

PC privacy concerns, AVE
average variance extracted

Rönkkö and Cho (2022) (see online Appendix D, Table D2). All construct correlations are lower than the root of AVE, thus supporting the Fornell-Larcker criterion (Hair et al. 2019). In addition, all HTMT ratios are far below the threshold of 0.90 and all CI_{CFA} values are below the threshold of 0.80, thus indicating that our research constructs are statistically different from each other (Henseler et al. 2015).

We also assessed convergent and discriminant validity of the three trust components. While ability, benevolence, and integrity demonstrate convergent validity (see online Appendix I, Table I3), the results revealed limited discriminant validity between benevolence and integrity according to the Fornell-Larcker criterion (see online Appendix I, Table I4). This, again, can be attributed to the nature of ability, benevolence and integrity being components of trust as an overarching concept. A post-hoc analysis of trust and its components is provided in Sect. 4.6, to gain more insight into these relationships.

3.4 Data Analysis Procedure

After having established measurement model validity, we followed a two-stage approach to estimate the parameters of our structural model and performed a multigroup analysis. The two-stage approach first determines the standardized latent variable factor scores for each construct by estimating the measurement model. These factor scores can then be employed in subsequent analyses such as moderation and subgroup analyses (Henseler et al. 2010). The two-stage procedure is an adequate one since, in our conceptualization, the measurement model is conceptualized as being invariant of the provider group. Consequently, factor scores were utilized for the subgroup analyses and for the assessment of the structural model. To mitigate model complexity issues with the given sample size, the control variables were tested separately. All calculations were performed in SPSS 22 (IBM 2013) and SmartPLS 4.0 (Ringle et al. 2022).

4 Results

We first tested the hypothesized provider governance differences in trust and its components (H1), before assessing the structural model and performing a multigroup analysis to test hypotheses H2-H4 of our research model (see Fig. 1).

4.1 Provider Governance Differences in Trust

The group means and subgroup means in trust, its components, and intention to use are displayed in Table 4, along with their respective test results for mean differences. Note that these factor scores are normalized (i.e., $M = 0$ and $SD = 1$ for the full sample). To test for differences on a group level (i.e., public versus private provider governance), we employed t -tests for independent samples. To test for differences on a subgroup level (i.e., provider types: health authority, public insurance, big company, startup), we performed an ANOVA multigroup analysis using Fisher's least significant difference (LSD) post-hoc tests. Fisher's LSD tests works like a t -test for multiple groups in that it uses the pooled standard deviation from all the groups, which gives it more statistical power compared to other post-hoc comparison methods (Williams and Abdi 2010).

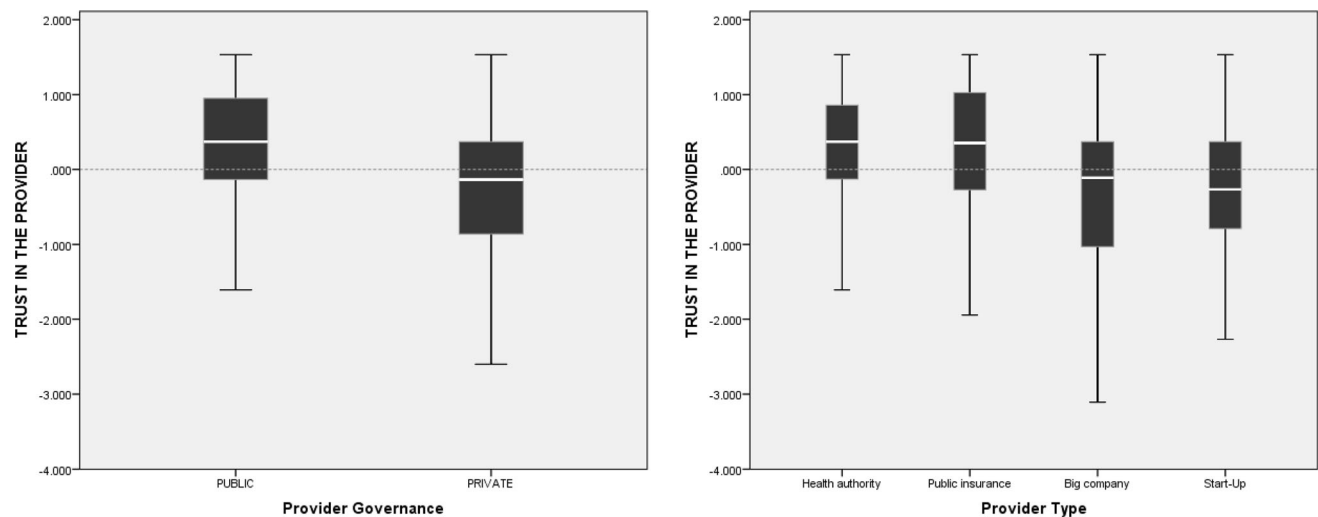
Regarding differences in *trust in the provider*, we find evidence for significant differences in the group means. Group means are significantly higher for public providers than for private providers (0.289, -0.324, $t = 5.346$, $p < 0.001$). This confirms H1: Trust in public providers is higher than trust in private providers. The post-hoc tests on a subgroup level provide a more detailed picture. Not only are the means significantly higher for the health authority and public insurance scenarios (0.295, 0.284, respectively) than for big company and startup scenarios, the mean for the big company scenario (-0.368) is also lower than for the startup scenario (-0.273), though not significantly. Figure 3

Table 4 Group and subgroup means and differences (T-Tests and ANOVA)

	Means public (Health Auth. Pub. Insurance)	Means private (Big Company Startup)	Group difference p (t)	Significant subgroup differences ^a
Trust	0.289 (0.295 0.284)	-0.324 (-0.368 -0.273)	0.613*** (5.346)	H > B, H > S, I > B, I > S
Ability	-0.043 (-0.283 0.189)	0.048 (0.028 0.069)	-0.09 (-0.76)	H < I, H < B, H < S
Benevolence	0.191 (0.229 0.155)	-0.214 (-0.370 -0.037)	0.406*** (3.485)	H > B, I > B, B < S
Integrity	0.170 (0.185 0.155)	-0.190 (-0.076 -0.189)	0.360*** (3.080)	H > B, I > B
Intention to use	0.115 (0.208 0.026)	-0.129 (-0.076 -0.189)	0.244** (2.070)	H > S

H health authority, I insurance, B big company; S startup | * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$ (two-sided)

^aANOVA post-hoc LSD test

**Fig. 3** Boxplot of trust in the provider for *Provider Governance* and *provider type*

illustrates these group and subgroup differences through boxplots.

While this finding of trust in the provider is broadly consistent with its trust components of *benevolence* and *integrity*, there are significant differences between public and private providers in the expected direction (see Table 4). However, it is worth noting that for *ability*, the differences between the provider governance groups are practically in the opposite direction (-0.043 for public, 0.048 for private), though not significantly. An intriguing observation emerges when analyzing the subgroup differences based on the provider type. Both private providers (i.e., big companies and startups) are attributed with a considerable level of ability in the area of PHR apps. However, health authorities are considered to be the least

capable (-0.283), while public insurances are attributed with the highest ability (0.189) (online Appendix F offers boxplots for benevolence, integrity, and ability).

To explore how the differences in trust and its components translate into usage intentions (the dependent variable), Table 4 also provides (sub)group test results for *intention to use*. It shows that the means are significantly higher for public providers (0.115) than for private providers (-0.129, $t = 2.070$, $p < 0.01$). The subgroup test unveils that the health authority and insurance apps receive the highest intention to use (0.208, 0.026, respectively), while the subgroup means for the big company and startup company scenarios are lower (-0.076, -0.189, respectively), although these subgroup differences are only significant

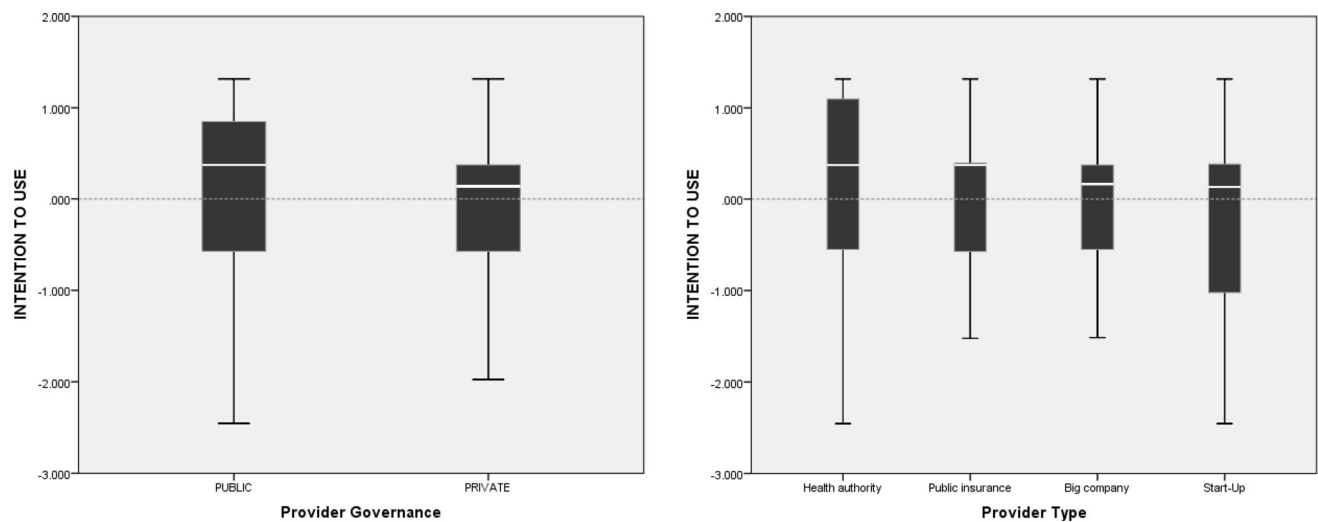


Fig. 4 Boxplot of intention to use for *Provider Governance* and *provider type*

between the health authority and the startup types. Figure 4 illustrates these (sub)group differences in intention to use.

Overall, our results support hypothesis H1 for trust, indicating that the type of provider governance (whether public or private) significantly influences the level of trust that users place in the app provider. Specifically, our results show that users tend to have higher levels of trust in public providers of a health record app, while they perceive private providers as less trustworthy. This difference extends to the *benevolence* and *integrity* components of trust. However, the hypothesized difference does not hold for *ability*. Here, we found significant subgroup differences, with health authorities showing significantly lower levels of ability compared to all other groups (public insurances, big companies, startups). These nuanced findings may explain the measurement issues surrounding ability as a trust component and highlight the variations across provider types.

4.2 Structural Model Assessment and Pathways

Before proceeding with the examination of our research hypotheses concerning the differential pathways between trust and intentions to use a PHR app, it is essential to assess the validity of the structural model. We used the entire sample (i.e., public and private provider scenarios) and employed bootstrap analysis with 10,000 samples to this end. Table 5 presents the results of the structural model tests, including the results for the public and private provider subgroups. In addition to the significance levels of these path coefficients (β), we report the p -values obtained from the subgroup analyses (i.e., t -test (Chin 2000) and multigroup analysis (Sarstedt et al. 2011)), which allow for

an assessment of the statistical significance of the differences between the provider governance groups.

We find that all paths between the endogenous constructs demonstrate statistical significance and align with our expected directions. This provides evidence for the three pathways in which trust in the provider translates into usage intentions, namely through perceived benefits, perceived risks, and through perceived control. The total effects of trust on intention to use confirm that trust significantly influences the intention to use ($\beta = 0.44^{***}$, $t = 8.92$, Table 5). Considering the control variables, only *willingness to disclose* exerted a significant influence on intention to use the mobile health app.

4.3 Path Analysis for Public and Private Providers

Having established the existence of three different pathways through which trust translates into usage intentions, we now shift our focus to the analysis of the hypothesized indirect effects of provider governance (H2–H4). The multigroup analysis focuses on examining the differences in the path coefficients in the public versus private provider subsamples (see Table 5 and Fig. G1 in online Appendix G).

Regarding the indirect effect of trust on intention to use via perceived benefits, our results demonstrate a significantly stronger effect for private providers ($\beta = 0.35^{***}$, $t = 5.31$) than for public providers ($\beta = 0.18^{**}$, $t = 3.03$, $p = 0.031$). Thus, our findings provide support for hypothesis H2; provider governance alters the pathway in which trust translates into usage intentions via perceived benefits. Additionally, when looking at the direct effects between trust \rightarrow perceived benefits, and perceived benefits \rightarrow intention to use, we find that all paths are significant

Table 5 Results of the model tests: main effects and total (indirect) effects

	Hypothesis	Path	Full sample (<i>n</i> = 286)	Public (<i>n</i> ₁ = 151)	Private (<i>n</i> ₂ = 135)	Group differences		Results
						<i>t</i> -test	MGA ^b	
						<i>p</i>	<i>p</i>	
Direct effects	–	Trust → Perceived benefits	0.54*** (10.55)	0.42*** (6.00)	0.67*** (12.31)	0.003	0.003	–
	–	Trust → Perceived risks	-0.65*** (13.84)	-0.65*** (12.45)	-0.68*** (8.93)	0.357	0.346	–
	–	Trust → Perceived control	0.60*** (12.65)	0.48*** (6.64)	0.73*** (16.52)	0.002	0.001	–
	–	Perceived benefits → Intention to use	0.46*** (6.86)	0.42*** (4.37)	0.52*** (6.37)	0.236	0.232	–
	–	Perceived risks → Intention to use	-0.16* (2.22)	-0.27** (3.05)	0.004 (0.04)	0.021	0.022	–
	–	Perceived control → Intention to use	0.15** (2.58)	0.05 (0.64)	0.27** (3.20)	0.026	0.026	–
Total and indirect effects	–	Trust → Intention to use	0.44*** (8.92)	0.38*** (6.51)	0.55*** (7.64)	0.033	0.039	–
	H2 (<)	Trust → Perceived benefits → Intention to use	0.25*** (4.99)	0.18** (3.03)	0.35*** (5.31)	0.029	0.031	Supported
	H3 (<)	Trust → Perceived risks → Intention to use	0.10* (2.08)	0.18** (2.81)	0.00 (0.04)	0.030	0.031	Reversed
	H4 (<)	Trust → Perceived control → Intention to use	0.09** (2.42)	0.02 (0.63)	0.20** (3.00)	0.009	0.009	Supported
Paths (Controls)	–	Privacy awareness → Intention to use	-0.06 (1.08)	-0.04 (0.40)	-0.05 (0.87)	0.434	0.440	–
	–	PC collection → Intention to use	-0.02 (0.36)	-0.01 (0.06)	-0.04 (0.53)	0.373	0.373	–
	–	PC error → Intention to use	0.00 (0.10)	0.03 (0.57)	-0.03 (0.45)	0.234	0.236	–
	–	PC unauth. access → Intention to use	-0.04 (0.97)	-0.03 (0.43)	-0.05 (0.79)	0.430	0.430	–
	–	Willingness to disclose → Intention to use	0.16* (2.15)	0.21* (1.85)	0.07 (0.66)	0.192	0.193	–
	–	Gender → Intention to use	0.01 (0.14)	0.06 (0.83)	-0.01 (0.13)	0.237	0.214	–
	–	Age → Intention to use	-0.05 (0.91)	0.04 (0.68)	-0.13 (1.55)	0.047	0.048	–
	–	Education → Intention to use	0.02 (0.47)	0.06 (0.92)	0.00 (0.02)	0.247	0.247	–
	–	Frequency of app use → Intention to use	-0.01 (0.17)	0.00 (0.02)	0.01 (0.09)	0.486	0.488	–
	–	Insurance → Intention to use	-0.17 (0.93)	-0.03 (0.13)	-0.34 (1.01)	0.204	0.212	–
	–	R ² (Intention to use)	0.437	0.401	0.497	–	–	–
	–	R ² adj. (Intention to use)	0.431	0.389	0.485	–	–	–

n.s. not supported; ^bMGA multigroup analysis (one-sided comparison); **p* < .05; ***p* < .01; ****p* < .001;

To adhere to model sample size the control variables were tested separately

in both groups. As expected, the effect of trust on perceived benefits is significantly stronger for private providers ($\beta = 0.67^{***}$, $t = 12.31$) than for public providers ($\beta = 0.42^{***}$, $t = 6.00$, $p = 0.003$). The effect of perceived benefits on intention to use is also stronger for private providers ($\beta = 0.52^{***}$, $t = 6.37$) than for public providers ($\beta = 0.42^{***}$, $t = 4.37$), although this difference is not significant.

Concerning the pathway through perceived risks, our results reveal a surprising finding: The indirect path of trust on intention to use via perceived risks is not only significantly stronger for public providers ($\beta = 0.18^{**}$, $t = 2.81$) than for private providers ($\beta = 0.00$, $t = 0.04$, $p = 0.031$), but this indirect effect is not significant at all for private providers. While this provides evidence that provider governance alters the pathway in which trust translates into usage intentions via perceived risks, it is the opposite of what we had hypothesized. Therefore, the results do not support hypothesis H3. A closer look at the direct effects between trust \rightarrow perceived risks, and perceived risks \rightarrow intention to use shows that the negative effect of trust on perceived risks is significant for both, public providers ($\beta = -0.65^{***}$, $t = 12.45$) and private providers ($\beta = -0.68^{***}$, $t = 8.93$), without a significant group difference. However, the effect of perceived risks on intention to use is only significant for the public group ($\beta = -0.27^{**}$, $t = 3.05$), but not for the private group ($\beta = 0.004$, $t = 0.04$, $p = 0.022$).

Turning to perceived control, we find evidence that the indirect path of trust on intention to use is significantly stronger for private providers ($\beta = 0.20^{**}$, $t = 3.00$) than for public providers ($\beta = 0.02$, $t = 0.63$, $p = 0.009$), for which the indirect effect is absent. Thus, our findings support hypothesis H4; provider governance alters the pathway in which trust translates into usage intentions via perceived control. Looking at the direct paths, the results show that the effect of trust on perceived control is significantly stronger for private providers ($\beta = 0.73^{***}$, $t = 16.52$) than for public providers ($\beta = 0.48^{***}$, $t = 6.64$, $p = 0.001$). The effect of perceived control on intention to use is not only significantly stronger for private providers ($\beta = 0.27^{**}$, $t = 3.20$), but there is no effect at all for public providers ($\beta = 0.05$, $t = 0.64$, $p = 0.026$).

The analysis of the total effect of trust on intention to use summarizes these findings by showing that the total effects are significantly stronger for private providers ($\beta = 0.55^{***}$, $t = 7.64$) than for public providers ($\beta = 0.38^{***}$, $t = 6.51$, $p = 0.039$). As to control variables, we find that willingness to disclose had a significant effect on intention to use in the full sample and for public providers ($\beta = 0.21^*$, $t = 1.85$), although without a significant group difference. Regarding group differences, only the effect of age on intention to use was significantly different

between the public provider and private provider groups ($p = 0.048$), but neither path was significant for either group (public: $\beta = 0.04$; private: $\beta = -0.13$). For all other control variables, no significant paths or group differences were detected.

4.4 Regression of Usage Intentions on Download Decisions

Regarding the download decision (whether a participant wanted to proceed with the download or not), we conducted a logistic regression including the intention to use and all control variables as predictors. The results showed a moderate to strong relationship of the model predictors with the download decision, as indicated by the Nagelkerke and Cox-Snell pseudo R^2 values of 0.509 and 0.375, respectively. The intention to use emerges as the strongest and significant predictor of the decision to download the app ($B = 1.577$, Wald statistics = 49.827, $p < 0.001$). Examining the odds ratios, an increase of one standard deviation in the intention to use made a user 4.84 times more likely to decide to download the PHR app in our experiment (95% CI [3.13, 7.50]), regardless of the provider type. Furthermore, the willingness to disclose personal data also influenced the download decision ($B = 0.536$, Wald statistics = 5.590, $p = 0.18$) with an odds ratio of 1.709 (95% CI [1.10, 2.66]). The logistic regression model correctly predicted 85.7% of cases with a positive download decision and 69.4% of cases with a negative download decision, resulting in an overall prediction accuracy of 79.4%.¹

4.5 Post-hoc Mediation Analysis

Our structural model revealed three indirect effects of trust on intention to use, namely through perceived benefits, perceived risks and perceived control. Following Zhao (2010), we also conducted a post hoc mediation analysis to understand the extent to which these indirect effects mediate a possible direct effect of trust on intention to use. We estimated two different models to test for possible mediation. First, we analyzed the three variables in separate models to extract the mediating effect of each individual potential mediator. The total effect of trust on intention to use was significant with a coefficient of $\beta = 0.578$ ($t = 11.859$, $p < 0.001$), and the direct effects were $\beta = 0.338$ ($t = 5.934$, $p < 0.001$) for the path via perceived benefits, $\beta = 0.445$ ($t = 6.648$, $p < 0.001$) for the path via perceived risks, and $\beta = 0.462$ ($t = 8.195$, $p < 0.001$) for the path via perceived control. Regarding the indirect effects, all paths were significant with

¹ More comprehensive results are provided in online Appendix H.

$\beta = 0.240$ ($t = 5.364$, $p < 0.001$), $\beta = 0.132$ ($t = 2.591$, $p = 0.005$), and $\beta = 0.116$ ($t = 3.219$, $p = 0.001$) respectively. These results show that when considered individually, all three constructs partially mediate the effect of trust on intention to use, perceived benefits mediating 42%, perceived risks 23%, and perceived control 20% of the total effect.

Second, we estimated a mediation model according to Hair et al. (2022) that included all three potential mediators simultaneously. Here, the total effect of trust on intention to use was significant with a coefficient of $\beta = 0.589$ ($t = 11.856$, $p < 0.001$) and the direct effect of trust on intention to use when including all three mediators was significant with a coefficient of $\beta = 0.284$ ($t = 4.301$, $p < 0.001$). Regarding the indirect effects, perceived benefits partially mediated the effect of trust on intention to use ($\beta = 0.224$, $t = 4.888$, $p < 0.001$) with 39% of the total effect, while the indirect effects of perceived risks and perceived control were insignificant (see Table 6). This was as expected, because high correlations between the mediating constructs lead to an omission of the competing effects (see Table C1). That is, the presence of more mediators masks the effect of other potential mediators when considered simultaneously (Hair et al. 2022).

4.6 Post-hoc Analysis of Trust and Its Components

We conducted a second post-hoc analysis to investigate how *ability*, *benevolence*, and *integrity* influence the overall trust of individuals in an app provider, and analyzed the relationships between the constructs more in depth (see Figure I1 in online Appendix I). After applying the consistent PLS algorithm, R^2 in trust was 0.736 (adjusted: 0.733), indicating that almost three quarters of the variance in these components is shared with trust. For the full dataset, we found that the effects of benevolence on trust and those of integrity on trust were statistically significant ($\beta = 0.39^{***}$, $t = 7.43$ and $\beta = 0.50^{***}$, $t = 9.33$ respectively). The path coefficient of ability on trust was close to zero ($\beta = 0.018$) and lacked statistical significance (see Table 7), suggesting that ability does not contribute to trust in a health app provider in the context of this study. When analyzing the public and private datasets separately, the paths between benevolence and integrity on trust are significant for both groups, and multigroup analyses reveal no significant difference between them. However, the path of ability on trust in the app provider becomes significant only for the private group ($\beta = 0.13^*$, $t = 2.03$), and not for the public group, although multigroup analysis reveals that this difference is not significant.

5 Discussion

In the light of the ongoing debate surrounding adequate governance approaches to the digitalization of healthcare, the objective of this research was to examine whether and how provider governance has a bearing on the behavioral intention to use a mobile health app and the consequent decision of consumers to download such an app. By means of an online experiment using the case of a newly developed PHR app, we found that whether the provider of the health app is a public or a private institution matters not only for the perceived trustworthiness of this provider, but also for the intentions to use the health app and thus, in turn, for the decision to download it. Drawing on privacy calculus and privacy control perspectives, we developed three hypotheses that capture the differential effects in the strength of the pathways by which trust translates into usage intentions through perceived benefits, perceived risks, and perceived privacy control.

Specifically, we examined provider governance not only as a direct influence on trust (H1), but also as a moderator of the effects of trust on intention to use through perceived benefits (H2), perceived risks (H3), and perceived privacy control (H4). Our findings show that, while trust in private app providers is significantly lower than in public providers providing the same app, trust has a stronger positive total effect on the intention use through perceived benefits and perceived control for private providers than for public providers. Contrary to H3, however, the effect through perceived risks is stronger for public providers than for private providers. Overall, our study holds two important implications for privacy calculus theory and healthcare IS.

5.1 Implication 1: Towards a Sectoral Theory of Privacy Calculus and Control

Our study represents a first step towards a sectoral theory of privacy calculus and privacy control that accounts for the contextual differences in private versus public sectors. Our research thus subscribes to the calls that context matters in the study of trust and privacy phenomena (e.g., Acquisti et al. 2015; Bansal et al. 2016; Chong et al. 2022; Yun et al. 2019). Privacy calculus theory has received widespread attention since the early 2000s in the context of e-commerce research. Since then, it has been used in different areas concerning consumer trust in online interactions with businesses, including social networking (Yun et al. 2019). It is therefore not surprising that the overwhelming majority of privacy studies in IS have (implicitly) taken a private sector context as a premise. Privacy in the highly regulated field of healthcare, however, is arguably more complex than in the traditional playing field of privacy research. This is because, depending on the

Table 6 Mediation analysis

Total effects (T → IU)		Direct effect (T → IU)			Indirect effects (T → IU)			Mediation	
Coefficient (T-value)	p-value	Coefficient (T-value)	p-value	Path	Coefficient (T-Value)	p-value	Percentile bootstrap 95% confidence interval		
							5% lower bound	95% upper bound	
0.578 (11.856)	0.000	0.338 (5.934)	0.000	$T \rightarrow PB \rightarrow IU$	0.240 (5.364)	0.000	0.169	0.317	Yes, partial
		0.445 (6.648)	0.000	$T \rightarrow PR \rightarrow IU$	0.132 (2.591)	0.005	0.054	0.222	Yes, partial
		0.462 (8.195)	0.000	$T \rightarrow PC \rightarrow IU$	0.116 (3.291)	0.001	0.062	0.177	Yes, partial
		0.284 (4.301)	0.000	$T \rightarrow PB \rightarrow IU$	0.224 (4.888)	0.000	0.151	0.302	Yes, partial
				$T \rightarrow PR \rightarrow IU$	0.030 (0.633)	0.263	-0.042	0.112	No
				$T \rightarrow PC \rightarrow IU$	0.040 (1.156)	0.124	-0.016	0.099	No

Numbers in *Italics* are the results of simple mediation analyses

Table 7 Results of the post-hoc analysis of trust and its components

Path		Full sample ($n = 286$)	Public ($n_1 = 151$)	Private ($n_2 = 135$)	Subgroup analysis	
					t-test p	MGA ^b p
Paths	Ability → Trust in the provider	0.02 (0.32)	0.01 (0.10)	0.13* (2.03)	0.145	0.138
	Benevolence → Trust in the provider	0.39*** (7.43)	0.35*** (5.52)	0.38*** (5.12)	0.391	0.385
	Integrity → Trust in the provider	0.50*** (9.33)	0.52*** (7.10)	0.45*** (5.41)	0.270	0.254
	R ² (Trust in the provider)	0.736	0.691	0.774	–	–
	R ² adj. (Trust in the provider)	0.733	0.684	0.769	–	–

^bMGA multigroup analysis (one-sided comparison); * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

national health system context, in healthcare there are multiple (public and private) institutions involved in providing healthcare services and processing consumer data (Dash et al. 2019). Moreover, this data can have different levels of sensitivity (Rahman 2019). Previous research in healthcare has considered privacy calculus in either private sector (e.g., Li et al. 2014) or in public sector (e.g., Princi and Krämer 2020) contexts. The differences between trust and privacy in the interaction with public institutions and private companies, however, have to date not been adequately reflected in the healthcare IS literature. In this spirit, our study supports theory portability of privacy

calculus and privacy control theory to the field of healthcare IS.

Our support for the hypothesis that trust has a significantly stronger effect on intention to use via perceived benefits when the provider is a private company as opposed to a public institution (H2) is a first element of this sectoral theory. This finding means that for private providers of health apps, trust is essential to support the perception of consumer benefits, such as improved access to health data, support of their health literacy, better healthcare quality, and improved communication with physicians. Conversely, for a public app provider, consumers base their

expectations of benefits to a much lesser extent on their trust in this provider. Our theoretical explanation for this sectoral difference is grounded in institutional trust perspective and a proposed effect of public regulation as a trust-enhancing and trust-substituting mechanism. During the Covid-19 pandemic, for example, consumers adopted tracing apps more widely when they were recommended or even mandated by government regulation (Riemer et al. 2020). Our data show that, while consumers put greater trust in public providers, they have on average the same level of perceived benefits from the public provider's app as they do from the private provider's app. Usage intentions are, again, significantly lower with the private provider's app (Table 4). Our sectoral results suggest that, even if consumers lose trust in the public providers, this will hardly harm the benefit expectations and usage of the app to the same extent as it would for the private provider. It is thus likely that consumers base their benefit expectation of health apps by public providers on other beliefs than trust, such as the belief in the provider's mission to contribute to the public good (Galetsi et al. 2023; Lounsbury et al. 2021).

The second element of our differential theory of privacy calculus and privacy control can be seen in the findings regarding H4. Trust has a significantly stronger effect on intention to use via perceived control when the provider is a private company; the effect is insignificant when the provider is public (Table 5). Perceived control relates to the belief that the individual can control which other parties (e.g., physicians, insurances, third parties) obtain access to the data, and for which purposes. The perception that consumers can control their privacy when interacting online has been confirmed as an important criterion that drives IS usage intentions, including those in a healthcare context (e.g., Princi and Krämer 2020). Here, we do not only see an indication for public governance acting as a trust-substituting, but also as a control-substituting mechanism. For private providers, consumers believe to have this control only if they trust the provider. For public providers, in contrast, trust is not a prerequisite to the same extent. More important, however, is the second leg of the pathway. Perceived control does not seem to be a relevant criterion for users to anchor their usage intentions when the provider is public. To put it differently, for public health apps, consumers do not seem to prioritize the presence of privacy controls in their decision to adopt the app, while for private health apps they do. This suggests that public providers are not expected to provide the same level of privacy controls as private providers.

The third and last element of a sectoral privacy calculus theory is given by our unexpected findings regarding hypothesis H3: Trust has a stronger effect on intention to use via perceived risks when the provider is public than

when it is private; the effect is insignificant, when the provider is private. This finding is surprising as one could have expected the level of regulation inherent to public governance to have the same trust substitution effect for perceived risks as for the perceived benefits and controls. Delving deeper into this path, it is evident that the lack of significance observed for private providers can be attributed to the insignificant direct effect of perceived risk on intention to use (Table 5). In other words, for private providers, privacy risks did not have an effect on intention to use the health app evaluated in our study. On the one hand, this finding contrasts with the literature that has found perceived risks as a central predictor of usage intentions in private sector contexts, including in healthcare (e.g., Li et al. 2014; Nicolaou and McKnight 2006). One possible explanation could be that the high risks inherent to the context of healthcare data are already factored into users' intentions, regardless of the perception of these risks. An alternative explanation could be that in the light of the comparatively high perceived benefits of healthcare apps from private providers, potential users of health apps base their calculus solely on these benefits and tend to disregard the risks. Further research is warranted to explore which of these possible explanations holds true for private providers of health apps. On the other hand, the privacy risk part of the calculus turns out to be highly relevant for apps from public providers. Hence, risk perceptions can apparently not be mitigated through regulation and public governance. It might be rooted in the psychology of the individual that fears of data loss and data misuse cannot be mitigated by the fact that the other party is a trusted and regulated institution (Lounsbury et al. 2021). The perceived lesser ability of public providers might imply that users may be particularly concerned about their data being compromised by third parties if it is stored with public providers. Overall, our H3 finding contributes to the debate on policy approaches in healthcare digitalization by teasing out a new boundary of public governance for health technology adoption. Users apparently need to trust public institutions as much as they need to trust private institutions to become convinced that their data is securely and privately stored, and this perception is even more crucial here for their usage intentions than with private providers.

In sum, our findings suggest that private providers of mobile health services can translate users' trust into usage intentions by strengthening the benefits and control perceptions of their health apps. Public providers, in contrast, can proactively strive to attract users by addressing and lowering the perceived risks of their offerings. The overarching theoretical implication is that we provide a nuanced picture of how privacy calculus and privacy control theory apply to public sector healthcare IS as opposed to the predominantly studied setting in private

sector (i.e., business) contexts. Public governance and regulation act as partial substitutes for trust in relation to the positive drivers of usage intentions while exacerbating the role of perceived risks, as our sectoral privacy calculus and privacy control perspective suggests.

5.2 Implication 2: Reconsidering Ability as a Trust Component

Second, our study questions the notion of ability as a necessary component of institutional trust, particularly in the context of healthcare digitalization. Previous trust research in IS has conceptualized ability, defined as the competencies, skills, and task-related activities that enable the trustee to succeed in a specific domain (Becker et al. 2014), as one of the three important components of institutional trust, next to benevolence and integrity (Mayer et al. 1995). Although this tripartite conceptualization has received wide recognition, researchers have also encountered problems with its operationalization. For example, Söllner et al. (2010) found that integrity was not a significant trust component in the context of mobile phone services. In our study of mobile health apps, ability did not prove to be a significant component of trust in a mobile health provider, although both constructs, trust and ability, taken by themselves demonstrated psychometric validity.

We argue that the non-significance of ability in the context of trust in a mobile health app provider, as demonstrated in our post-hoc analysis, is not a product of randomness or error, but indicative of the dilemma we face in the healthcare context, specifically in the market like the one that was studied (Germany). While consumers still have relatively high trust in public authorities and believe in their integrity and benevolence, they have somewhat lost faith in the government's capability to effectively deliver mobile health services, such as a PHR, to all citizens. This sentiment is clearly reflected in the subgroup means for H1, where trust in the public health authority significantly surpasses that in both private providers, while perceived ability of the public health authority is significantly lower than that of both private types (and also lower than the public insurance type, see Table 4). Germany, in particular, has a history of slow progress in healthcare digitalization with regards to publicly provided infrastructure (Blümel et al. 2020; Retiene 2022).

While ability was not associated with trust for public providers, we found a weak association for private providers (Table 7). The key theoretical implication is that institutional trust and ability are not always and in any case correlated. This challenges the assumption that institutional trust can be universally specified through the three components of ability, integrity, and benevolence. Thus, there is a need to be aware of the context when studying the

components that potentially form trust in institutions and providers of health IS services. In healthcare digitalization, consumers may trust certain parties although they do not consider them as able (e.g., governments), while conversely, they might distrust others (e.g., companies), whom they perceive as more competent in delivering effective digital health services. Thus, our research unveils a novel trust-ability dilemma in the context of healthcare digitalization that warrants future exploration.

5.3 Limitations

The generalizability of the research implications is constrained by the following limitations. First, since healthcare is an inherently complex field subject to specific cultural and regulatory conditions, we focused on one specific market (Germany) and one specific app (a PHR) to keep these conditions constant. Trust in public versus private organizations and its relative effects on usage intentions might be weighed differently by users from other national contexts, depending on the specific mobile health app. Second, we deliberately excluded healthcare providers as a provider type, since healthcare providers (e.g., hospitals) are unlikely to provide PHR apps in the market that was studied (Germany). Third, although we included a set of control variables, there is a possibility that additional variables outside the scope of this study could have an effect on the intention to use a PHR.

Fourth, while our sample was fairly balanced in terms of gender, the average age of the participants was relatively young, with 31.4 years. A more balanced sample in terms of age distribution may have yielded different results. Fifth, to operationalize the two provider governance types for the purpose of our online experiment, we chose four specific entities and labels. Although we have argued how and why each of these entities adequately represents the two governance types, it is possible that participants of our experiments would have rated the study variables differently, had we chosen other entities and labels. Sixth, our sample was acquired using the online platform Prolific, which may imply certain self-selection biases to our sample beyond the factors we were able to control for.

Seventh, participants of our study were exposed to a simulated PHR app that was presented to them as a genuine app under development, which may limit the external validity of our research. Eighth, our study uses downloading as a proxy for app usage, mainly highlighting initial adoption of PHR apps and neglecting to understand long-term usage. Future research should explore what drives both initial downloads and ongoing, effective use of PHR apps for (sensitive) health data management. Lastly, our cross-sectional user data only ascertains statistical

association, not the causality that is inherent to our theorizing and hypotheses.

5.4 Practical Implications

Similar to many other countries, the recent plans in Germany to expand the nationwide health infrastructure through PHRs (the ePA) have sparked ongoing debates concerning the potential benefits and risks, with adoption levels remaining minimal (Schrahe 2021). The findings of our study advocate that public stakeholders step up their efforts to promote the implementation and provision of nationwide PHRs through publicly governed digital infrastructures. Despite a frequently noted institutional trust paradox (Rothstein and Stolle 2008), our research demonstrates that users in Germany place significantly higher levels of trust in public providers to manage their personal health data compared to private companies, including big companies and startups. These findings starkly contrast with studies conducted in other countries, such as the US, that have evidenced distrust toward government involvement in the sharing of health data (Anderson and Agarwal 2011). Hence, our research reinforces the notion that in the sphere of European healthcare, publicly regulated providers are viewed as the most reliable stewards of health data.

Second, our study informs public *and* private providers about the mechanisms through which they can sustain and increase people's intentions to adopt mobile health apps. In particular, private providers should prioritize the promotion of the application's health management benefits and its privacy controls. Conversely, public providers ought to concentrate their efforts on addressing the perceived risks associated with the application. Regarding the German ePA implementation, it stands to reason that insufficient information about the measures to mitigate privacy and security threats may have been one of the key factors that hindered the widespread acceptance of the PHR in Germany in the past. In this sense, we hope that our study can provide an impetus for stakeholders to design more user-centric PHR apps and complement these with effective communication strategies for a positive change.

6 Conclusions

Mobile health apps play a crucial role in the future provision of care, with a notable surge in the number of publicly and privately governed apps entering the market. In an effort to investigate how app provider governance influences PHR usage intentions, this study developed a sectoral theory of privacy calculus and perceived control, which was tested in an online experiment with a sample of

potential users of a PHR app in Germany. Our results provide evidence of a partially trust-substituting effect in public sector: While public providers exhibit higher levels of trust and lower levels of ability than private providers, this trust alone is not as crucial for creating perceived benefit and control expectations in users as it is for private providers. However, trust remains a more critical factor for mitigating perceived privacy and security risks for public providers than for private providers. In addition to contributing to the ongoing debate regarding the governance for health technology adoption, our research also challenges the assumption that trust is always associated with ability, particularly in a public sector context. Healthcare regulators and app providers can glean insights from our study regarding the technology and communication levers through which they can effectively enhance the widespread acceptance and usage of their mobile health offerings.

Supplementary Information The online version contains supplementary material available at <https://doi.org/10.1007/s12599-024-00869-4>.

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Abd-alrazaq AA, Bewick BM, Farragher T, Gardner P (2019) Factors that affect the use of electronic personal health records among patients: a systematic review. *Int J Med Inform* 126:164–175. <https://doi.org/10.1016/j.ijmedinf.2019.03.014>
- Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* 347:509–514. <https://doi.org/10.1126/science.aaa1465>
- Adjerid I, Acquisti A, Telang R, Padman R, Adler-Milstein J (2016) The impact of privacy regulation and technology incentives: the case of health information exchanges. *Manag Sci* 62:1042–1063. <https://doi.org/10.1287/mnsc.2015.2194>
- Ajzen I (1985) From intentions to actions: a theory of planned behavior. In: Kuhl J, Beckmann J (eds) *Action control: from cognition to behavior*. Springer, Heidelberg, pp 11–39

- Ajzen I (1991) The theory of planned behavior. *Organ Behav Hum Decis Proc* 50:179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Anderson CL, Agarwal R (2011) The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Inf Syst Res* 22:469–490. <https://doi.org/10.1287/isre.1100.0335>
- Angst CM, Agarwal R (2009) Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. *MIS Q* 33:339–370. <https://doi.org/10.2307/20650295>
- Appenzeller A (2020) Privacy and patient involvement in e-health worldwide: an international analysis. In: Beyerer J, Zander T (eds) *Proceedings of the 2020 Joint workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory*, pp 1–17
- Archer N, Fevrier-Thomas U, Lokker C, McKibbin KA, Straus SE (2011) Personal health records: a scoping review. *J Am Med Inform Assoc* 18:515–522. <https://doi.org/10.1136/amiajn-2011-000105>
- Arundel A, Bloch C, Ferguson B (2019) Advancing innovation in the public sector: aligning innovation measurement with policy goals. *Res Policy* 48:789–798. <https://doi.org/10.1016/j.respol.2018.12.001>
- Balasubramanian S (2022) Google's healthcare data platform, Care Studio, is partnering with one of the largest EHR systems. <https://www.forbes.com/sites/saibala/2022/03/20/googles-health-care-data-platform-care-studio-is-partnering-with-one-of-the-largest-ehr-systems/>. Accessed 25 Apr 2024
- Bandyopadhyay S, Ozdemir Z, Barron JM (2012) The future of personal health records in the presence of misaligned incentives. *Commun Assoc Inf Syst* 31:155–166. <https://doi.org/10.17705/ICAIS.03107>
- Bansal G, Zahedi FM, Gefen D (2016) Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Inf Manag* 53:1–21. <https://doi.org/10.1016/j.im.2015.08.001>
- Bartol J, Prevodnik K, Vehovar V, Petrovčič A (2022) The roles of perceived privacy control, Internet privacy concerns and Internet skills in the direct and indirect Internet uses of older adults: conceptual integration and empirical testing of a theoretical model. *New Media Soc.* <https://doi.org/10.1177/14614448221122734>
- Becker J, Heddier M, Öksüz A, Knackstedt R (2014) The effect of providing visualizations in privacy policies on trust in data privacy and security. In: *Proceedings of the 47th Hawaii international conference on system sciences (HICSS)*, pp 3224–3233
- Bellman S, Johnson EJ, Kobrin SJ, Lohse GL (2004) International differences in information privacy concerns: a global survey of consumers. *Inf Soc* 20(5):313–324. <https://doi.org/10.1080/01972240490507956>
- Blümel M, Spranger A, Achstetter K, Maresso A, Busse R (2020) Germany: health system review. *Health Syst Transit* 22:1–272
- Brandimarte L, Acquisti A, Loewenstein G (2013) Misplaced confidences. *Soc Psychol Pers Sci* 4:340–347. <https://doi.org/10.1177/1948550612455931>
- Buhr L, Schickntanz S, Nordmeyer E (2022) Attitudes toward mobile apps for pandemic research among smartphone users in Germany: national survey. *JMIR Mhealth Uhealth* 10:e31857. <https://doi.org/10.2196/31857>
- Bundesministerium für Gesundheit (2023) Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz-DigiG). <https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/digig>. Accessed 25 Apr 2024
- Carter L, Bélanger F (2005) The utilization of e-government services: citizen trust, innovation and acceptance factors. *Inf Syst J* 15:5–25. <https://doi.org/10.1111/j.1365-2575.2005.00183.x>
- Chin WW (2000) Multi-group analysis with PLS. <http://disc-nt.cba.uh.edu/chin/plsfaq/multigroup.htm>. Accessed 15 Apr 2024
- Chong AYL, Blut M, Zheng S (2022) Factors influencing the acceptance of healthcare information technologies: a meta-analysis. *Inf Manag* 59:103604. <https://doi.org/10.1016/j.im.2022.103604>
- Connolly R, Sanchez OP, Compeau D, Tacco F (2023) Understanding engagement in online health communities: a trust-based perspective. *J Assoc Inf Syst* 24:345–378. <https://doi.org/10.17705/Ijais.00785>
- Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organ Sci* 10:104–115. <https://doi.org/10.1287/orsc.10.1.104>
- Culnan MJ, Bies RJ (2003) Consumer privacy: balancing economic and justice considerations. *J Soc Issues* 59:323–342. <https://doi.org/10.1111/1540-4560.00067>
- Dash S, Shakyawar SK, Sharma M, Kaushik S (2019) Big data in healthcare: management, analysis and future prospects. *J Big Data* 6:1–25. <https://doi.org/10.1186/s40537-019-0217-0>
- Davis FD, Bagozzi RP, Warshaw PR (1989) User acceptance of computer technology: a comparison of two theoretical models. *Manag Sci* 35:982–1003. <https://doi.org/10.1287/mnsc.35.8.982>
- Deuker A (2010) Addressing the privacy paradox by expanded privacy awareness—the example of context-aware services. *Privacy and identity management for life. IFIP International Federation for Information Processing, Berlin*, pp 275–283
- Dinev T, Hart P (2005) Internet privacy concerns and social awareness as determinants of intention to transact. *Int J Electron Commer* 10:7–29. <https://doi.org/10.2753/JEC1086-4415100201>
- Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inf Syst Res* 17:61–80. <https://doi.org/10.1287/isre.1060.0080>
- Dinev T, Hart P, Mullen MR (2008) Internet privacy concerns and beliefs about government surveillance—an empirical investigation. *J Strateg Inf Syst* 17:214–233. <https://doi.org/10.1016/j.jsis.2007.09.002>
- Dinev T, Albano V, Xu H, D'Atri A, Hart P (2016) Individuals' attitudes towards electronic health records: a privacy calculus perspective. In: Gupta A et al (eds) *Advances in healthcare informatics and analytics*, vol 19. Springer, Cham, pp 19–50. https://doi.org/10.1007/978-3-319-23294-2_2
- Ebert TAE (2009) Facets of trust in relationships—a literature synthesis of highly ranked trust articles. *J Bus Mark Manag* 3:65–84. <https://doi.org/10.1007/s12087-008-0034-9>
- Ehrari H, Ulrich F, Andersen HB (2020) Concerns and trade-offs in information technology acceptance: the balance between the requirement for privacy and the desire for safety. *Commun Assoc Inf Syst* 47:227–247. <https://doi.org/10.17705/ICAIS.04711>
- Eling N, Krasnova H, Widjaja T, Buxmann P (2013) Will you accept an app? Empirical investigation of the decisional calculus behind the adoption of applications on Facebook. In: *Proceedings of the 34th international conference on information systems (ICIS)*
- Entreß-Fürsteneck M von, Buchwald A, Urbach N (2019) Will I or will I not? Explaining the willingness to disclose personal self-tracking data to a health insurance company. In: Bui T (ed) *Proceedings of the 52nd Hawaii international conference on system sciences (HICSS)*, pp 1351–1361
- Featherman MS, Pavlou PA (2003) Predicting e-services adoption: a perceived risk facets perspective. *Int J Hum-Comput Stud* 59:451–474. [https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)

- Fink L (2022) Why and how online experiments can benefit information systems research. *J Assoc Inf Syst* 23:1333–1346. <https://doi.org/10.17705/1jais.00787>
- Fishbein M, Ajzen I (1975) Belief, attitude, intention and behavior: an introduction to theory and research. Addison-Wesley, Reading
- Flavián C, Guinalíu M (2006) Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Ind Manag Data Syst* 106:601–620. <https://doi.org/10.1108/02635570610666403>
- Fox G, Lynn T, Rosati P (2022) Enhancing consumer perceptions of privacy and trust: a GDPR label perspective. *ITP* 35:181–204. <https://doi.org/10.1108/ITP-09-2021-0706>
- Galetsi P, Katsaliaki K, Kumar S (2023) Exploring benefits and ethical challenges in the rise of mHealth (mobile healthcare) technology for the common good: an analysis of mobile applications for health specialists. *Technovation* 121:102598. <https://doi.org/10.1016/j.technovation.2022.102598>
- Gefen D, Straub D (2003) Managing user trust in B2C e-services. *e-Service J* 2:7–24. <https://doi.org/10.1353/esj.2003.0011>
- Gematik (2022) Über uns | Gematik. <https://www.gematik.de/ueber-uns>. Accessed 15 Jan 2024
- George JF, Kohnke E (2018) Personal health record systems as boundary objects. *Commun Assoc Inf Syst* 42:2. <https://doi.org/10.17705/1CAIS.04202>
- Gokgoz ZA, Ataman MB, van Bruggen GH (2021) There's an app for that! understanding the drivers of mobile application downloads. *J Bus Res* 123:423–437. <https://doi.org/10.1016/j.jbusres.2020.10.006>
- Gong Z, Han Z, Li X, Yu C, Reinhardt JD (2019) Factors influencing the adoption of online health consultation services: the role of subjective norm, trust, perceived benefit, and offline habit. *Front Publ Health* 7:286. <https://doi.org/10.3389/fpubh.2019.00286>
- Google Health (2023) Care studio: clinical software to unify healthcare data. <https://health.google/caregivers/care-studio/>. Accessed 19 Jan 2024
- Hair JF, Risher JJ, Sarstedt M, Ringle CM (2019) When to use and how to report the results of PLS-SEM. *Eur Bus Rev* 31:2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- GKV Spitzenverband (2023) Die gesetzlichen Krankenkassen. https://www.gkv-spitzenverband.de/krankenversicherung/kv_grundprinzipien/alle_gesetzlichen_krankenkassen/alle_gesetzlichen_krankenkassen.jsp. Accessed 15 Jan 2024
- Hair JF, Hult GTM, Ringle CM, Sarstedt M (2022) A primer on partial least squares structural equation modeling (PLS-SEM). Sage, Thousand Oaks
- Harris MA, Brookshire R, Chin AG (2016) Identifying factors influencing consumers' intent to install mobile applications. *Inf J Inf Manag* 36:441–450. <https://doi.org/10.1016/j.ijinfomgt.2016.02.004>
- Henseler J, Fassott G (2010) Testing moderating effects in PLS path models: an illustration of available procedures. In: Esposito Vinzi V et al (eds) *Handbook of partial least squares: concepts, methods and applications*. Springer, Heidelberg, pp 713–735
- Henseler J, Ringle CM, Sarstedt M (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J Acad Mark Sci* 43:115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Hvidman U (2019) Citizens' evaluations of the public sector: evidence from two large-scale experiments. *J Publ Admin Res Theor* 29:255–267. <https://doi.org/10.1093/jopart/muy064>
- IBM (2013) IBM SPSS statistics for Windows. IBM Corp, Armonk
- Jarvenpaa SL, Tractinsky N, Vitale M (2000) Consumer trust in an Internet store. *Inf Technol Manage* 1:45–71. <https://doi.org/10.1023/A:1019104520776>
- Jensen TB, Thorseng AA, Jensen TB, Thorseng AA (2017) Building national healthcare infrastructure: the case of the Danish e-health portal. In: Aanestad M, et al (eds) *Information infrastructures within European health care*. Health informatics. Springer, Cham, pp 209–224. https://doi.org/10.1007/978-3-319-51020-0_13
- Jercich K (2021) Google has another go at patient health record software | Healthcare IT News. <https://www.healthcareitnews.com/news/google-has-another-go-patient-health-record-software>. Accessed 25 Apr 2024
- Judah R, D'Amico K, Radin J, Israel A, Leste T, Mahoney N, Gisby S (2020) New roads to the health innovation ecosystems of tomorrow. <https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/innovationecosystems-in-health-care.html>. Accessed 13 May 2024
- Kim DJ, Ferrin DL, Rao HR (2009) Trust and satisfaction, two stepping stones for successful e-commerce relationships: a longitudinal exploration. *Inf Syst Res* 20:237–257. <https://doi.org/10.1287/isre.1080.0188>
- Laufer RS, Wolfe M (1977) Privacy as a concept and a social issue: a multidimensional developmental theory. *J Soc Issues* 33:22–42. <https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>
- Lee J, Park Y-T, Park YR, Lee J-H (2021) Review of national-level personal health records in advanced countries. *Healthc Inform Res* 27:102–109. <https://doi.org/10.4258/hir.2021.27.2.102>
- Li H, Gupta A, Zhang J, Sarathy R (2014) Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decis Support Syst* 57:376–386. <https://doi.org/10.1016/j.dss.2012.10.043>
- Lin J, Carter L, Liu D (2021) Privacy concerns and digital government: exploring citizen willingness to adopt the COVID-Safe app. *Eur J Inf Syst* 30:389–402. <https://doi.org/10.1080/0960085X.2021.1920857>
- Lounsbury O, Roberts L, Goodman JR, Batey P, Naar L, Flott KM, Lawrence-Jones A, Ghafur S, Darzi A, Neves AL (2021) Opening a “can of worms” to explore the public's hopes and fears about health care data sharing: qualitative study. *J Med Internet Res* 23:e22744. <https://doi.org/10.2196/22744>
- MacKenzie S, Podsakoff P, Podsakoff N (2011) Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. *MIS Q* 35:293–334
- Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Inf Syst Res* 15:336–355. <https://doi.org/10.1287/isre.1040.0032>
- Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organizational trust. *Acad Manag Rev* 20:709
- McKnight DH, Choudhury V, Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Inf Syst Res* 13:334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- MedWatcher (2023) Home | MedWatcher. <https://en.medwatcher.io/>. Accessed 25 Apr 2024
- Miller AR, Tucker C (2009) Privacy protection and technology diffusion: the case of electronic medical records. *Manag Sci* 55:1077–1093. <https://doi.org/10.1287/mnsc.1090.1014>
- Mittendorf C (2017) The implications of trust in the sharing economy—an empirical analysis of Uber. In: *Proceedings of the 50th Hawaii international conference on system sciences (HICSS)*, pp 5837–5846
- Mou J, Cohen J (2014) Trust, risk barriers and health beliefs in consumer acceptance of online health services. In: *Proceedings of the 35th international conference on information systems (ICIS)*
- Niazhani Z, Toni E, Cheshmekaboodi M, Georgiou A, Pirnejad H (2020) Barriers to patient, provider, and caregiver adoption and use of electronic personal health records in chronic care: a

- systematic review. *BMC Med Inform Decis Mak* 20:153. <https://doi.org/10.1186/s12911-020-01159-1>
- Nicolaou AI, McKnight DH (2006) Perceived information quality in data exchanges: effects on risk, trust, and intention to use. *Inf Syst Res* 17:332–351. <https://doi.org/10.1287/isre.1060.0103>
- O'Mara M (2015) 3 Reasons why Google health failed. <https://web.archive.org/web/20230605173651/https://www.recordations.com/blog/3-reasons-why-google-health-failed/>. Accessed 25 Apr 2023
- Parmar H, Tahvildar A, Ghasemi E, Jung S, Davis F, Walden E (2022) To download or not to download? Spatial and temporal neural dynamics across the brain regions when deciding to download an app. *Inf J Inf Manag* 66:102531. <https://doi.org/10.1016/j.ijinfomgt.2022.102531>
- Pavlou PA (2003) Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *Int J Electron Commer* 7:101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Pavlou PA, Gefen D (2004) Building effective online marketplaces with institution-based trust. *Inf Syst Res* 15:37–59. <https://doi.org/10.1287/isre.1040.0015>
- Peer E, Rothschild D, Gordon A, Evernden Z, Damer E (2021) Data quality of platforms and panels for online behavioral research. *Behav Res Meth* 54:1643–1662. <https://doi.org/10.3758/s13428-021-01694-3>
- Pentina I, Zhang L, Bata H, Chen Y (2016) Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. *Comput Hum Behav* 65:409–419. <https://doi.org/10.1016/j.chb.2016.09.005>
- Pesce NL (2020) Americans trust Amazon and Google more than the police or the government – MarketWatch. <https://www.marketwatch.com/story/people-trust-amazon-and-google-more-than-the-police-or-the-government-2020-01-14>. Accessed 15 Apr 2024
- Ploner N, Neurath MF, Schoenthaler M, Zielke A, Prokosch H-U (2019) Concept to gain trust for a German personal health record system using public cloud and FHIR. *J Biomed Inform* 95:103212. <https://doi.org/10.1016/j.jbi.2019.103212>
- Princi E, Krämer NC (2020) Out of control–privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Front Psychol* 11:1–15. <https://doi.org/10.3389/fpsyg.2020.582054>
- Rahman MS (2019) Does privacy matters when we are sick? An extended privacy calculus model for healthcare technology adoption behavior. In: 2019 10th International conference on information and communication systems, Irbid. IEEE, Piscataway, pp 41–46. <https://doi.org/10.1109/IACS.2019.8809175>
- Rainey H, Fernandez S, Malatesta D (2021) Understanding and managing public organizations, 6th edn. Wiley, Boston
- Retiene R (2022) Health-related activities of Big Tech. Munich Personal RePEc Archive. MPRA Paper No. 115080:1–167. <https://mpra.ub.uni-muenchen.de/115080/>
- Riemer K, Ciriello R, Peter S, Schlagwein D (2020) Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. *Eur J Inf Syst* 29:731–745. <https://doi.org/10.1080/0960085X.2020.1819898>
- Ringle CM, Wende S, Becker J-M (2022) SmartPLS 4. SmartPLS, Oststeinbek. <https://www.smartpls.com>. Accessed 25 Apr 2024
- Robin R, Dandis AO (2021) Business as usual through contact tracing app: what influences intention to download? *J Mark Manag* 37:1903–1932. <https://doi.org/10.1080/0267257X.2021.2017323>
- Roehrs A, Da Costa CA, Da Rosa RR, de Oliveira KSF (2017) Personal health records: a systematic literature review. *J Med Internet Res* 19:e5876–e5876. <https://doi.org/10.2196/jmir.5876>
- Rönkkö M, Cho E (2022) An Updated Guideline for Assessing Discriminant Validity. *Organ Res Methods* 25:6–14. <https://doi.org/10.1177/1094428120968614>
- Rothstein B, Stolle D (2008) The state and social capital: an institutional theory of generalized trust. *Comp Politics* 40:441–459. <https://doi.org/10.5129/001041508X12911362383354>
- Saengchai S, Sriyakul T, Jemsittiparsert K (2020) The impact of citizen trust, citizen disposition and favourable social characteristics on the adoption of eGovernment: mediating roles of perceived behavioural control. *Int J Innov Creat Change* 12:375–393
- Sarstedt M, Henseler J, Ringle CM (2011) Multigroup analysis in partial least squares (PLS) path modeling: alternative methods and empirical results. In: Sarstedt M, et al (eds) *Measurement and research methods in international marketing*, vol 22. Emerald, Chennai, pp 195–218. [https://doi.org/10.1108/S1474-7979\(2011\)0000022012](https://doi.org/10.1108/S1474-7979(2011)0000022012)
- Schrahe D (2021) EHR against the background of the legislation-the unconventional German way. *Gesundheitsökonomie Und Qualitätsmanagement* 26:310–316. <https://doi.org/10.1055/a-1521-5431>
- Sheeran P (2002) Intention–behavior relations: a conceptual and empirical review. *Eur Rev Soc Psychol* 12:1–36. <https://doi.org/10.1080/14792772143000003>
- Shin D-H (2009) Towards an understanding of the consumer acceptance of mobile wallet. *Comput Hum Behav* 25:1343–1354. <https://doi.org/10.1016/j.chb.2009.06.001>
- Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Q* 20:167–195. <https://doi.org/10.2307/249477>
- Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. *MIS Q* 35:989–1015. <https://doi.org/10.2307/41409970>
- Söllner M, Hoffmann A, Leimeister JM (2016b) Why different trust relationships matter for information systems users. *Eur J Inf Syst* 25:274–287. <https://doi.org/10.1057/ejis.2015.17>
- Söllner M, Leimeister JM (2013) What we really know about antecedents of trust: a critical review of the empirical information systems literature on trust. In: *Psychology of trust: new research*, pp 127–155
- Söllner M, Axel Hoffmann, Hirdes EM, Rudakova L, Leimeister S, Leimeister J (2010) Towards a formative measurement model for trust. In: *BLED 2010 proceedings*
- Söllner M, Benbasat I, Gefen D, Leimeister JM, Pavlou PA (2016a) Trust. <https://www.misqresearchcurations.org/blog/2017/5/10/trust-1>. Accessed 10 Jan 2024
- Söllner M (2020) Same same but different? A Two-Foci perspective on trust in information systems. In: *Proceedings of the 53rd Hawaii international conference on system sciences (HICSS)*, pp 5129–5138
- Soper DS (2024) A-priori Sample Size Calculator for Structural Equation Models. <https://www.danielsoper.com/statcalc/calculator.aspx?id=89>. Accessed 24 Jan 2024
- Spil T, Klein R (2015) The personal health future. *Health Policy Technol* 4:131–136. <https://doi.org/10.1016/j.hlpt.2015.02.004>
- Statista (2024) Größte gesetzliche Krankenkassen in Deutschland nach der Mitgliederanzahl in den Jahren 2016 bis 2020. <https://de.statista.com/statistik/daten/studie/856392/umfrage/groesste-gesetzliche-krankenkassen-indeutschland-nach-der-versicherten-zahl/>. Accessed 13 May 2024
- Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ (2006) Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *J Am Med Inform Assoc* 13:121–126. <https://doi.org/10.1197/jamia.M2025>

- Tertulino R, Antunes N, Morais H (2023) Privacy in electronic health records: a systematic mapping study. *J Public Health*. <https://doi.org/10.1007/s10389-022-01795-z>
- Venkatesh V, Morris MG, Davis GB, Davis FD (2003) User acceptance of information technology: toward a unified view. *MIS Q* 27:425–478. <https://doi.org/10.2307/30036540>
- Walker KL (2016) Surrendering information through the looking glass: transparency, trust, and protection. *J Publ Policy Mark* 35:144–158. <https://doi.org/10.1509/jppm.15.020>
- Ward PR, Miller E, Pearce AR, Meyer SB (2016) Predictors and extent of institutional trust in government, banks, the media and religious organisations: evidence from cross-sectional surveys in six Asia-Pacific countries. *PLoS ONE* 11:e0164096. <https://doi.org/10.1371/journal.pone.0164096>
- Webb TL, Sheeran P (2006) Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychol Bull* 132:249–268. <https://doi.org/10.1037/0033-2909.132.2.249>
- Williams LJ, Abdi H (2010) Fisher's least significant difference (LSD) test. In: Salkind N (ed) *Encyclopedia of research design*. Sage, Thousand Oaks
- Wottrich VM, van Reijmersdal EA, Smit EG (2018) The privacy trade-off for mobile app downloads: the roles of app value, intrusiveness, and privacy concerns. *Decis Support Syst* 106:44–52. <https://doi.org/10.1016/j.dss.2017.12.003>
- Wu J, Du H (2012) Toward a better understanding of behavioral intention and system usage constructs. *Eur J Inf Syst* 21:680–698. <https://doi.org/10.1057/ejis.2012.15>
- Xu H, Dinev T, Smith HJ, Hart P (2008) Examining the formation of individual's privacy concerns: toward an integrative view. In: *Proceedings of the 29th international conference on information systems (ICIS)*
- Yun H, Lee G, Kim DJ (2019) A chronological review of empirical research on personal information privacy concerns: an analysis of contexts and research constructs. *Inf Manag* 56:570–601. <https://doi.org/10.1016/j.im.2018.10.001>
- Zion Market Research (2023) Personal health record software market growth, size, share, trends, and forecast 2030. <https://www.zionmarketresearch.com/report/personal-health-record-software-market-size>. Accessed 4 Apr 2024