Who will Users Entrust with Their Personal Health Records?
An Online Experiment on the Effects of the Provider Type

Personal health records (PHRs) are a key element in the digitalization of healthcare. This research addresses the underexplored question of whether a PHR app provider is public or private has an effect on the behavioral intentions to use and download PHR apps. We designed an online experiment that presents potential users with a PHR app that is randomly stated to be provided either by a health authority, a public insurance, a Big Tech, or a startup. Subsequently, the participants will be surveyed for their usage intentions, trust in the provider, perceived benefits, and perceived risks of this app. Our planned contribution is to add an institutional trust perspective to privacy calculus theory that considers public versus private app provider types.

Introduction

Over the last years, countries around the world have accelerated the process of digitizing healthcare. In this development, personal health records (PHR) are regarded as a key technology to support personal health management (Tang et al., 2006). PHRs, which are *digital platforms through which individuals can access, manage and share their personal health information in a private, secure, and confidential environment* (Tang et al., 2006), face pervasive challenges across most nations (Roehrs et al., 2017). Despite pertinent privacy regulations (e.g., HIPAA, GDPR), trust in PHR providers remains a major issue as the "idea to maintain one's personal health information electronically has [yet] failed to takeoff among consumers" (Spil & Klein, 2015). Prior research has intensively studied the factors that influence the acceptance of information technologies (IT) and highlighted the role of privacy-related factors, such as trust (e.g., Carter & Bélanger, 2005; Lin et al., 2021) and privacy concerns (e.g., Dinev & Hart, 2005; Malhotra et al., 2004). While trust has consistently been found to have a positive impact on the intention to use an app, perceptions of privacy risks or security risks were widely found to decrease it.

What is largely unknown, however, is the influence of the provider of a health app on the user's intention to use it. Previous research has shown that people have different levels of trust in different institutions

(Ward et al., 2016). In general, there is an institutional trust paradox: Although public institutions rely on the trust of the people to effectively act as their agents (Rothstein & Stolle, 2008), consumers in many countries trust private companies more than their governments (Pesce, 2020; Ward et al., 2016). It yet stands to evaluate whether this trust paradox also holds for the storing of sensitive health data in PHRs. Understanding the impact of the app provider type (i.e., public versus private) on people's perceptions of trust, privacy, and usage intentions in healthcare could be a key to solve the persistent PHR trust challenges. Therefore, this paper aims to address the question: *How does the app provider type influence the behavioral intention to use and the decision to download a personal health records app?*

Related Work and Hypothesis Development

So far, only a limited number of studies have put emphasis on potential differences between app providers (e.g., Anderson & Agarwal, 2011; Bansal et al., 2016; Jarvenpaa et al., 2000). Taking our vantage point in an institutional trust perspective, we first hypothesize the influence of public (i.e., health authority and public insurance) versus private (i.e., Big Tech and startup) **app provider types on trust**. We consider four potential types of app providers, of which two are private and two are public. *Health authorities* are governmental bodies that make health-related policy and provide oversight of the health sector. *Public insurances* are corporations under public law that carry out tasks of public interest (e.g., reimbursing health services) and are therefore highly regulated, but legally independent entities. *Big Techs* are publicly listed companies under corporate law that are viewed to have an accountability beyond financial terms also for issues such as social responsibility. *Startup* companies include new ventures and smaller companies that develop and provide PHR solutions. We assume that public institutions have a high degree of accountability, since it is their mandate to serve the population (Rothstein & Stolle, 2008), while many private companies focus on making profit. Therefore, we hypothesize that: ***H1****: The app provider type will influence the trust in the PHR app provider. Specifically, trust in public providers will be higher than trust in private providers.* Based on previous research outcomes (e.g., Carter & Bélanger, 2005; Gefen & Straub,

2003), we further expect to see the following mediating effect: ***H1m****: Trust in the app provider mediates the effect of app provider type on the intention to use a PHR app.*

We next draw on **privacy calculus theory** which is a widely accepted model that presumes that individuals make privacy decisions based on the net outcome of weighing the anticipated benefits and risks of this decision (Culnan & Bies, 2003; Laufer & Wolfe, 1977). We conceptualize four possible **benefits of PHRs** from a user perspective: enabling access to personal health information, strengthening health literacy, improving healthcare quality, and enhancing communication between patients and physicians (Bandyopadhyay et al., 2012; Tang et al., 2006). While public institutions may be ascribed the power and long-term orientation that is necessary for a large-scale introduction of a PHR, private providers are seen as being more focused on profit than healthcare outcomes. Therefore, we hypothesize: ***H2****: The app provider type influences the perceived benefits of a PHR app, such that users will perceive higher benefits in apps provided by public providers and lower benefits in apps provided by private providers.* In addition, based on previous research outcomes (e.g., Gong et al., 2019; Li et al., 2014), we expect to see the following mediating effect: ***H2m****: Perceived benefits mediates the effect of app provider type on the intention to use a PHR app.* The second component of the privacy calculus consists of the **perceived risks** associated with a situation-specific decision. This threat comes in two main forms: the loss of data due to the intrusion of unauthorized third parties into the technical systems (i.e., perceived security risks) and the poor handling of personal information by the app provider (i.e., perceived privacy risks). We assume that people perceive the two types of risks differently depending on the app provider. Public institutions (should) act in the interest of the citizens and protect the sensitive data while private companies could profit from sharing personal health data for non-essential purposes. In sum, we hypothesize that: ***H3****: The app provider type influences the perceived risks of a PHR app, such that users will perceive lower risks in apps provided by public providers and higher risks in apps provided private providers.* Based on previous research outcomes (e.g., Li et al., 2014; Nicolaou & McKnight, 2006), we further expect to see the following mediating effect:

***H3m**: Perceived risks mediates the effect of app provider type on the intention to use a PHR app.* Figure 1 presents an overview of our hypotheses and the overall research model:

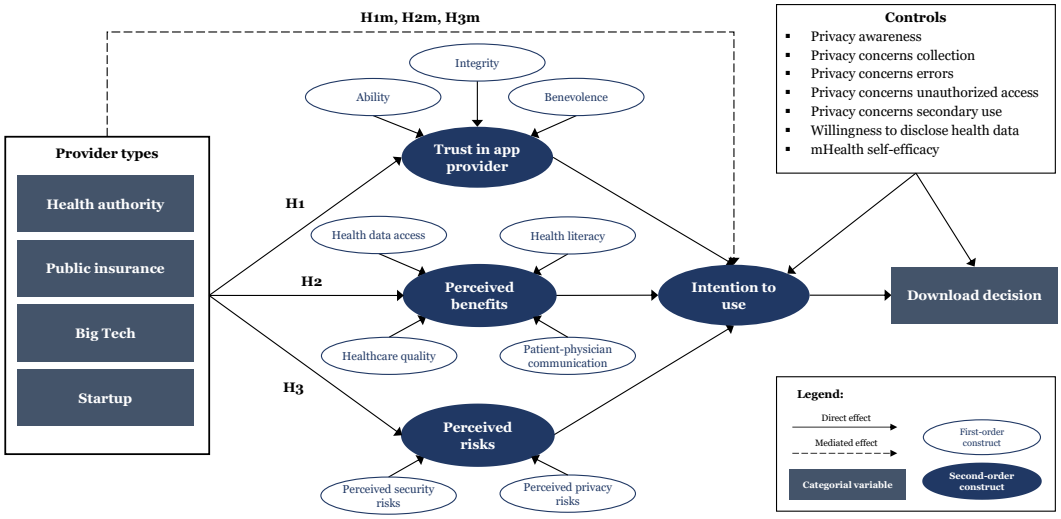

Figure 1. Research Model

Table 1 summarizes the constructs of this research. As control variables, we consider a number of general traits that can influence an individual's behavioral intentions to use, such as privacy awareness (Xu et al., 2008), privacy concerns (Smith et al., 2011), willingness to disclose personal health data (von Entreß-Fürsteneck et al., 2019), and m-health self-efficacy (Fox & Connolly, 2018).

Table 1. Research Constructs and Definitions

Construct	**Definition**	**Guiding References**
App provider type	Legal and economic nature of an institution developing and operating a PHR app	Self-developed
Intention to use	Behavioral intention to use a PHR app	Venkatesh et al., 2003 & self-developed
Trust in the app provider (ability, benevolence, integrity)	Trusting beliefs in a particular app provider and its attributes that are useful to the trustor	Gefen & Straub, 2003; Malhotra et al., 2004; McKnight et al., 2002 & self-developed
Perceived benefits (healthcare quality, health data access, patient-physician communication, health literacy)	Belief that the expected outcome of using the outlined PHR app is beneficial and valuable	Li et al., 2014; Tang et al., 2006 & self-developed
Perceived risks (perceived security risks, perceived privacy risks)	Belief that the expected outcome of using the PHR app is risky and bears loss potential	Dinev et al. 2006; Flavián & Guinalíu, 2006; Li et al., 2014 & self-developed

Methodology

We combine experimental research with survey methods. For the experiment, we developed an interactive click-prototype of a PHR app based on existing PHR apps on the German market, which we branded *MyHealthRecord*. Based on this template app, we branched out four variants that differ only by the displayed logo and data processor declarations (name and address) in the privacy statement. For reasons of external validity, we chose app providers that (could) realistically offer 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) and for the public insurance provider, we chose *Techniker Krankenkasse*, which is one of the largest statutory health insurances in Germany based on memberships (Statista, 2022). To represent the Big Tech provider type, we chose Siemens as a well-known German company that is active in health IT under its *Siemens Healthineers* brand. To represent the startup provider type, we invented a name, logo, and company background of a typical startup, which we labelled *digitalhealth labs*.

The items for our constructs in the research model were taken from existing literature (see Table 1) and adapted to our context whenever necessary and translated to German. All constructs are measured using 5-point Likert scales ranging from 'I do not agree' to 'I do agree'. In the online experiment, participants are presented with a short pre-introduction to the study background and are told that they will participate in a user study of a new PHR app that is under development. Participants are not informed in advance about the actual objective of our study in order to avoid biases regarding their attitudes towards the app. Study participants are then randomly assigned to one of the four app provider type scenarios. Following that, an introduction explaining the PHR app in more detail is shown, which includes some more background information about the respective app provider (e.g., headquarter location and number of employees). After reading the introduction, participants are presented with an interactive simulated app and are tasked to familiarize themselves with the app's functionalities. The survey asks about the participants' intentions to use and to download the app (yes/no) directly after interacting with the app to avoid any bias through privacy-related questions. After that, participants have to pass through the survey by rating the

aforementioned construct items. Additional questions about demography, frequency of health-related app usage, and health insurance membership are presented at the end of the survey. On the last page, we debrief the participants about the true purpose of the study.

Expected Contributions

Our results are expected to bring to light whether, to which extent, and through which mediators (provider trust, perceived benefits, perceived risks) the app provider type influences the behavioral intention to use and the decision to download a PHR app. Such knowledge should be helpful to assess whether there is an institutional trust paradox of consumers (in Germany) trusting private companies more than public institutions in healthcare technology. We plan to contribute to theory by examining institutional trust and the privacy calculus using an experimental setting in which causal inferences can be made regarding the effect of app provider type on trust, perceived risks, and perceived benefits.

From our participation in the 2022 HITS workshop, we hope to receive constructive feedback on our research design from the review process, based on which we are confident to be able to present first results from our online experiment at the venue in Copenhagen.

References

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. Information Systems Research, 22(3), 469–490.

Bandyopadhyay, S., Ozdemir, Z., & Barron, J. M. (2012). The Future of Personal Health Records in the Presence of Misaligned Incentives. Communications of the Association for Information Systems, 31(1), 7.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information & Management, 53(1), 1–21.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1), 5–25.

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues, 59(2), 323–342.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – a study of Italy and the United States. 15(4), 389–402.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10(2), 7–29.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. Industrial Management & Data Systems, 106(5), 601–620.

Fox, G., & Connolly, R. (2018). Mobile health technology adoption across generations: Narrowing the digital divide. Information Systems Journal, 28(6), 995–1019.

Gefen, D., & Straub, D. (2003). Managing User Trust in B2C e-Services. E-Service Journal, 2(2), 7–24.

Gong, Z., Han, Z., Li, X., Yu, C., & Reinhardt, J. D. (2019). Factors Influencing the Adoption of Online Health Consultation Services: The Role of Subjective Norm, Trust, Perceived Benefit, and Offline Habit. Frontiers in Public Health, 7, 286.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. Information Technology and Management 2000 1:1, 1(1), 45–71.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues, 33(3), 22–42.

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. Decision Support Systems, 57(1), 376–386.

Lin, J., Carter, L., Liu, D., Ågerfalk, P., Conboy, K., & Myers, M. (2021). Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app. European Journal of Information Systems, 30(4), 389–402.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336–355.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359.

Nicolaou, A. I., & McKnight, D. H. (2006). Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. Information Systems Research, 17(4), 332–351.

Pesce, N. L. (2020). Americans trust Amazon and Google more than the police or the government - MarketWatch. MarketWatch. https://www.marketwatch.com/story/people-trust-amazon-and-google-more-than-the-police-or-the-government-2020-01-14

Roehrs, A., da Costa, C. A., da Rosa Righi, R., & de Oliveira, K. S. F. (2017). Personal Health Records: A Systematic Literature Review. J Med Internet Res, 19(1), e5876.

Rothstein, B., & Stolle, D. (2008). The state and social capital: An institutional theory of generalized trust. Comparative Politics, 40(4).

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly, 35(4), 989–1015.

Spil, T., & Klein, R. (2015). The personal health future. Health Policy and Technology, 4(2), 131–136.

Statista. (2022). Größte gesetzliche Krankenkassen in Deutschland nach der Mitgliederanzahl in den Jahren 2016 bis 2020.

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. Journal of the American Medical Informatics Association, 13(2), 121–126.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

von Entreß-Fürsteneck, M., 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. Proceedings of the Annual Hawaii International Conference on System Sciences, 1351–1361.

Ward, P. R., Miller, E., Pearce, A. R., & Meyer, S. B. (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(10).

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. International Conference on Information Systems (ICIS).