Security and Privacy of Personal Health Records in Cloud Computing Environments – An Experimental Exploration of the Impact of Storage Solutions and Data Breaches

Michael Adelmeyer[1], Pascal Meier[1], and Frank Teuteberg[1]

[1] University of Osnabrück, Institute of Accounting and Information Systems, Germany
{michael.adelmeyer,pascal.meier,frank.teuteberg}@uos.de

Abstract. In the course of the digitization in healthcare, the collection and central storage of large health-related datasets in clouds in the form of personal health records is growing. However, the use of cloud services for sensitive data is associated with security and privacy risks. Further, the delegation of control over security and privacy measures to the cloud provider requires trust on the users' side. In order to investigate the role of security and privacy when storing and processing patient data, we conducted an online experiment, in which third-party cloud services are compared to private on-premise data centers. Additionally, we examine the impact of data breaches on the perceived security, privacy, control and trust in both storage scenarios. Our results indicate that cloud-based personal health records still face concerns regarding perceived security, privacy, control and trust amongst end-users. Nevertheless, after a data breach, no significant differences between both solutions exist.

Keywords: Cloud Computing, Personal Health Records, Security, Privacy.

1 Introduction

Personal health records (PHRs) can improve the collaboration between different healthcare actors and patients and ease the sharing of data [1] by providing central repositories of the users' state of health [2]. When providing PHRs for patients, cloud computing (CC) offers numerous benefits, such as scalable computing resources at minimal costs [3]. Yet, adopting CC services for sensitive health data introduces risks associated to security and privacy, as the data are stored externally or even in public environments, which entails additional challenges, such as access control or privacy protection [4], [5]. Compared to private on-premise data storage, the control over the data and corresponding security and privacy measures is delegated to the cloud provider, which requires trust in the capabilities of the provider on the users' side [4]. Since data security and privacy are crucial determinants for the adoption of PHRs [6], [7], it is necessary to evaluate whether patients' data should be stored and processed on-premise or externally, via scalable CC services. For PHR providers, the users'

14th International Conference on Wirtschaftsinformatik,
February 24-27, 2019, Siegen, Germany

acceptance, which is prerequisite for a sustainable adoption of the provided service, heavily depends on the selection of a secure and trustworthy storage solution [8].

Generally, data security and privacy issues are regarded as a central inhibitor for the adoption of cloud-based PHRs [5], [8]. For example, the cloud-based PHR app *vivy*, which was recently launched by several major German health insurances, faces massive criticism for data security and privacy issues, e.g., related to data hosting and processing at the underlying Amazon cloud platform [9]. Due to the high value and sensitivity of the data stored in PHRs, cloud environments are an attractive target of malicious attacks [5]. In case of a data breach, the security or privacy of the protected health data are compromised due to an impermissible use or disclosure [10]. The delegation of control in cloud environments [5], [11] and the corresponding need for trust [4] are connected to the perceived security and privacy of PHR users and in view of the theory of reasoned action [12], ultimately influencing the intention to use or adopt cloud-based PHRs [6]. Since CC faces skepticism [11], it is necessary to determine the importance of the factors that influence the intention to use cloud-based PHRs services to ensure their sustainable adoption. However, previous research either focuses on security or privacy related aspects [1], [5], [11], [13–15] or lacks a focus on either PHRs [11], [16] or CC [6], [7], [17]. Although data breaches continually impact the healthcare sector [5], [10], little research has been conducted on their outcome on users of cloud-based PHRs. Therefore, we adopt an experimental approach to investigate the participants' perceived security, perceived privacy, trust, perceived control and intention to use when using a PHR of a provider who stores and processes personal health data (a) at a cloud provider or (b) an on-premise data center. Additionally, the impact of data breaches on the targeted constructs is investigated. We examine the following research questions (RQ):

> *RQ1: Do patients' perceived security, perceived privacy, trust and perceived control differ between cloud environments and private on-premise data centers when storing personal health data in PHRs?*
> *RQ2: In case of a data breach, to which extent do patients' perceived security, perceived privacy, trust and perceived control differ when using cloud environments compared to private on-premise data centers?*

Based on the RQs, the study is structured as follows: First, hypotheses (H) targeting the above-mentioned constructs are derived from the literature. Second, the experimental approach and design are described. Afterwards, we analyze the collected data. In the conclusion, the findings are discussed.

2 Theoretical Background and Hypotheses Development

2.1 Data Security and Privacy

Although CC plays a significant role in healthcare, the technology still faces data security and privacy concerns, especially in PHR provisioning [8], [14], [15], [17], [18]. As the two concepts are strongly connected, individuals often may not fully understand the difference between security of systems and privacy of their data [19],

[20]. Individuals choose to disclose information, although this might impact their privacy [21], which is decisively based on trust and the perception of risks related to data security and privacy. Yet, individuals may decide to refrain from disclosures that would affect the security of their data [19]. Therefore, it is necessary to examine both concepts individually [19], which is not always the case in existing literature on cloud-based PHRs [13], [14]. Although multiple definitions exist, we adapt the most common-sense understanding of privacy [22] as an individual's ability to control the use of his or her own data [13], [20]. Besides perceived control [11], trust is a central determinant of users' intention to disclose information [21]. Whereas privacy focuses on individuals' control over their data, security is an overarching principle with focus on data confidentiality, integrity and availability [17]. Hence, in order to comply with privacy requirements, data security provides the technical foundations [18], [20].

Since certain information stored in PHRs is shared with multiple actors, risks for data security and privacy arise [15], [17]. Consequently, the infrastructure via which PHRs are provided should be rigorously secured [8], [17]. However, this is a central challenge for cloud environments, especially for public clouds [4], [14], [18], where the probability of unauthorized access to data is significantly higher compared to traditional systems [23]. Therefore, data security is of great importance for the provision of PHRs via cloud environments [1]. Hence, on the side of PHR and cloud service providers, extensive data security and privacy requirements must be considered to guarantee an equal level of data security compared to on-premise data centers [8]. Thus, we hypothesize that users' perceptions of security (SEC) and privacy (PRI) are more positive when PHRs are stored and processed on-premise, as using cloud services introduces additional risks and uncertainties [1], [4], [13], [24]:

H1a/H2a: The users' SEC/PRI is higher when their data are stored in on-premise data centers compared to cloud environments.

Despite the sensitivity of PHR data, the risks associated to CC and the higher probability of data disclosures in cloud environments [23], the impact of actual data breaches on users' SEC and PRI is only scarcely explored. If the security and privacy of users' personal health data were compromised in a data breach, this will likely lead to increased perceived risks and an increased motivation for protection [19]. Due to the value and sensitivity of health data stored in PHRs, data breaches occur frequently [10] and potential consequences are severe [13], regardless of the underlying storage solution. From the service users' perspective, the impact of and dealing with potential consequences are the same irrespective of whether a data breach occurred within a cloud or a conventional IT environment [23]. Thus, we hypothesize that the individuals' levels of SEC and PRI do not differ after a data breach:

H1b/H2b: After a data breach, the users' SEC/PRI is equal regardless of whether the data are stored in on-premise data centers or cloud environments.

2.2 Trust

Trust (TR) is defined 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 to the trustor, irrespective of the ability to monitor or control the trustee [25]. In the context of the acceptance of information systems, different trust targets exist, such as trust in a technology or a provider [26]. With regard to PHRs, the user takes the role of the trustor and the PHR provider the role of the trustee, who may utilize CC as underlying technology [24]. For the general adoption and use of cloud services, trust has been identified as a key factor [24], [27], as users delegate their control over data security and privacy to the provider, whose actions, in turn, are difficult to monitor [4]. In healthcare, users' trust in security and privacy mechanisms of cloud providers is seen as a core determinant [8], [13]. The trustor must be confident that the cloud technology adopted in a certain healthcare data sharing scenario complies with security and privacy requirements [18]. Hence, when storing and processing personal health data in a PHR, we conclude that users' trust in the PHR provider is lower when the data are stored in a cloud environment compared to on-premise data centers directly operated by the provider, since users perceive more risks associated to CC [11], [13], [16]. However, there should be no difference in the users' trust after a data breach, as the perceived risks and the corresponding lower trust levels towards the technology are superposed by the decrease of trust in the PHR provider [26]:

H3a: The users' TR is higher when their data are stored in on-premise data centers compared to cloud environments.

H3b: After a data breach, the users' TR is equal regardless of whether the data are stored in on-premise data centers or cloud environments.

Although most studies investigate the influence of perceived risks on trust [20], Mitchell (1999) identified that there is a bi-directional relationship between TR and perceived risks [28] that include SEC and PRI. This has, among others, been empirically proven by Hsin Chang and Wen Chen (2008) [29]. Regarding the acceptance of health clouds, trust in healthcare cloud providers and in privacy-preserving mechanisms influence the patients' information privacy concerns [13]. Thus, focusing on the role of security and privacy when storing personal health data in PHRs, we analyze the influence of TR on SEC and PRI:

H4/H5: The higher the users' TR, the higher the SEC/PRI.

2.3 Control

Another important aspect of privacy is the perceived control (CO) over a system or technology [30], which is largely determined by the extent to which a user is able to employ a system in order to achieve an intended goal [31]. In cloud environments, the users' control over data and privacy or security measures is largely delegated to the cloud provider [11], [24]. In consequence, users perceive lower control over their data, which is why they connect CC with insecurities [11]. Thus, CO additionally refers to the extent to which users perceive that they have an impact on the control over their activities and data in the cloud service used [32]. Due to the sensitivity of data stored in a PHR, it is necessary that the users perceive to be in control and to be able to decide over the access to and the usage of their data. In this context, CO aims at both internal and external control. This means that the user feels capable of using

the system and further, that the situation allows this [33]. Compared to on-premise data centers, the provision of PHRs via cloud environments mainly differs in terms of external control, since CC is afflicted with uncertainties regarding the security and privacy of data [4], [24]. However, in case of a data breach occurring at either storage solution, we hypothesize that the awareness of uncertainties and risks connected to CC services only plays a minor role, as a loss of control over information is regarded as material for the perception of a privacy invasion [11]. Consequently, the CO for both PHR data storing and processing solutions adjusts to a comparably low level:

H6a: The users' CO is higher when their data are stored in on-premise data centers compared to cloud environments.
H6b: After a data breach, the users' CO is equal regardless of whether the data are stored in on-premise data centers or cloud environments.

As trust is defined irrespectively of the ability to monitor or control the trustee [25], we do not assume a connection between CO and TR. Yet, SEC and PRI of PHRs are often linked to users' CO, for example, by implementing access controls for PHRs [17] or health data in clouds in order to increase data security and privacy [15]. In cloud environments, recent studies suggest that cloud users' CO majorly determines their PRI [11]. Hence, fostering users' CO by means of security and privacy measures enhances the users' SEC and PRI when storing and processing health data in PHRs:

H7/H8: The higher the users' CO, the higher the SEC/PRI.

2.4 Intention to Use

Following the theory of reasoned action, individuals' intentional behaviors to adopt or use a system are ultimately determined by their attitudes [12], [34]. The intention to use (ITU) can be defined as the intention of a customer or service user to (continually) use a provider and his service (also after an incident) [24], [32]. Besides a general attitude towards a service, the ITU of a person is measured based on risks and benefits regarding a scenario or technology [13], [24]. Due to the steadily increasing complexity of technology, trust plays a crucial role in the acceptance of and the ITU information systems [26], such as cloud environments. In view of the impact of users' security and privacy concerns towards CC, higher levels of security and privacy perceptions positively affect the ITU cloud services [16]. In this context, PRI and SEC are majorly determined by the delegation and the corresponding loss of control in cloud environments [11], [18], which ultimately affect the ITU cloud services [11]. In healthcare, control, trust, security and privacy are proven to influence the ITU cloud services, as end-users are not able to fully control the storage and processing of their data due to the control delegation and the opaque nature of cloud services [18], [24] as well as due to the sensitivity of data [13], [18]. Especially security and privacy are regarded as important requirements for the adoption of cloud-based PHRs [6], [8]. Further, trust is an antecedent of individuals' disclosure behavior [21]. Thus, it is assumed that SEC, TR, CO and PRI have a positive impact on the ITU in PHR data sharing scenarios:

H9/H10/H11/H12: The higher the users' SEC/TR/CO/PRI, the higher the ITU.

2.5 Research Model

The constructs and hypotheses are summarized in a research model (see Figure 1).

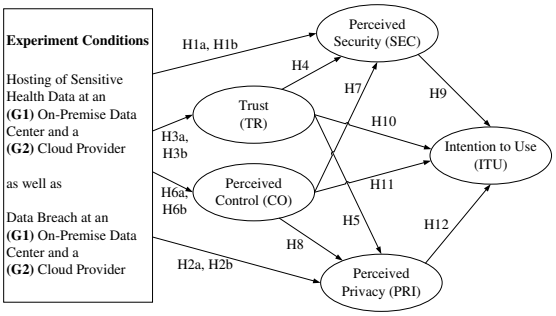

Figure 1. Research Model

3 Research Approach

3.1 Experimental Design and Procedure

In order to test the previously developed hypotheses, we conducted a web-based experiment using vignettes [35]. Overall, we applied a two-group posttest-only design [36], which was extended by an additional stimulus (X_2) and a second posttest (P_2) in both groups to determine the impact of a data breach on the outlined constructs. The overall procedure of the experiment is visualized in Figure 2.

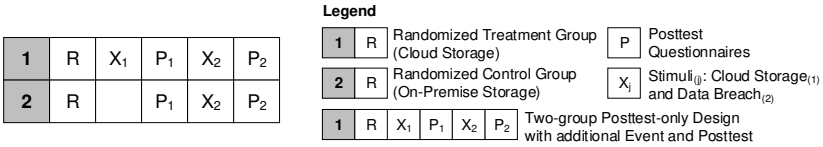

Figure 2. Experimental Setup

The random allocation (R) of the participants to the two experiment groups G1 and G2 took place in an unnoticeable first step of the experiment. Afterwards, a vignette was displayed, which can be described as a focused description of a hypothetical scenario that puts the subjects in a fictitious role in which they are asked to respond in certain ways [35]. Our vignette[1] introduced the participants to the German healthcare system, in which health-related data are stored decentrally. As a result, a medical treatment based on all existing health data is difficult, because stakeholders often cannot access all patient data. The participants are asked to act as longtime users of a service called *Vitalife*, which offers a PHR web service. The service provides a central storage and management of users' relevant personal health and related data. The first

[1] The full scenarios can be retrieved under the following link: http://bit.ly/WI-19

manipulation between group 1 (G1, treatment) and group 2 (G2, control) was conducted by using two data storage solutions of the PHR service provider *Vitalife*, i.e., a third-party cloud service (G1) (X_1) and a private on-premise data center directly operated by *Vitalife* (G2). The participants of both groups were identically informed about data security and privacy measures of the respective systems in use. Both storage solutions comply with common information security standards, such as ISO 27001, which require the development and implementation of a strict security program. Further, the third-party cloud service used by *Vitalife* complies with the cloud-related ISO 27017/27018 standards for IT security controls and the processing of personal data in cloud services. Both solutions offer an availability of 99.9 percent.

After the vignette, the first posttest (P_1) is conducted to measure the participants' attitudes towards the different storage solutions prior to a data breach. In the subsequent textual description of the event [24], [27] (X_2), the subjects are informed by *Vitalife's* customer service about a data breach at the employed cloud service provider (G1) or the on-premise data center (G2), in the course of which the PHR data of the participants were stolen. In both groups, an employee of *Vitalife* has been made responsible for the data breach, as he inadvertently opened a link in a phishing e-mail and thus enabled hackers to access the system. In order to allow for a comparison of the users' SEC, PRI, CO and TR before and after the data breach, a second identical posttest (P_2) was conducted directly after the event in both groups. In both tests, the participants were ultimately asked for their ITU the service based on their experience.

3.2 Operationalization of the Constructs

In the questionnaires, the subjects were surveyed regarding the outlined hypothetical constructs using several items derived from the literature (see Table 1).

Table 1. Constructs and Item Sources

Construct	*Adapted Definition*	*Source*
SEC	The perception of PHR service users regarding the capabilities of a provider to protect their data, which include safe transmission, prevention of unauthorized modification, access or interference.	[20]
PRI	The PHR service users' perceived ability to control the acquisition and use of their personal information [20], which includes the general concern of the provider, the adherence to privacy laws or the prevention of unauthorized information disclosure.	[20]
TR	The willingness of a PHR service user to be vulnerable to the actions of a PHR service provider, based on the expectation that the provider safely stores and provides patients' health data [25].	[37]
CO	The extent to which PHR service users perceive that they can impact the storing and processing of their health data as well as the access rights of other stakeholders to their data.	[31]
ITU	The intention to voluntarily use the provided PHR service, which stores health data in the cloud or in an on-premise data center.	[13], [32]

All items were measured by means of a seven-point Likert scale ranging from 1 ("strongly agree") to 7 ("strongly disagree"). For SEC and PRI, 6 items each from Flavián and Guinalíu (2006) [20] were used. TR was measured based on 11 items from McKnight et al. (2002) [37], with 4 items targeting the integrity (TRI) and ability (TRA) each as well as 3 items measuring the benevolence (TRB) of *Vitalife*. For CO, 4 items of Lee and Benbasat (2011) [31] were used. ITU was measured with 3 items adapted from Ermakova (2014) [13] and one from Walter et. al (2014) [32].

3.3 Participants and Data Collection

To test our proposed hypotheses, the previously described experimental concept was carried out as a web-based survey in February 2018. In total, 238 undergraduate economics and information systems students participated in the voluntary experiment, which was rewarded with minor raffled incentives. Out of the 238 answers, we only considered complete datasets for the analysis and eliminated answers with response patterns or significantly faster overall response times. Among the remaining 217 datasets, 104 participants belong to group 1 and 113 to group 2, with an overall of 35 % female and 65 % male participants and an average age of 20.6 years.

4 Data Analysis and Results

4.1 Construct Validity and Reliability

In order to ensure the validity and reliability of the collected data, several tests were conducted. The analysis of variances tests (ANOVA), Levene tests of variance equality and t-tests for the control variables gender, age, health condition and CC experience did not indicate significant differences between the groups (N = 217). Therefore, a homogeneous distribution of the participants can be assumed. Given a mean self-estimation of 3.37, it can be concluded that the participants are fairly knowledgeable in CC. Since most of the hypotheses and the research model are based on the first posttest, the validity and reliability are assessed based on the corresponding data and are thus concluded for the second posttest. The data were examined in order to preclude a common method bias (CMB) using Harman's one-factor test [38]. The 30 indicators used were examined in a factor analysis. Since the resulting extraction of one factor explaining 45.783% of the variance is below the threshold of 50%, we do not assume a CMB [38]. Subsequently, we assessed the one-dimensionality of the constructs in an exploratory factor analysis. All indicators meet the respective thresholds for Measure of Sampling Adequacy (MSA) (> .5), the Kaiser-Meyer-Olkin-criterion (KMO) (> .5), communalities (> .5) and the Bartlett-test (< .05) [39], except from the items TRB2 and TRB3 with communalities < .5 (.450 and .498). Hence, both items were dropped from further analyses, which, using reflective measurement, does not affect the meaning of a construct [39], [40]. Further, according to Kaiser's rule, five common factors with an eigenvalue of > 1, which explain 66.915% of the variance, could be extracted. This confirms our predetermined

five constructs SEC, PRI, CO, TR and ITU [39]. Although items with loadings > .6 are considered as reliable [41], we dropped all items with loadings < .7 in order to achieve better construct validity, as suggested by Nunnally and Bernstein (1994) [42]. This concerns our items TRA1 (.699), TRA4 (.576), PRI4 (.698) and SEC2 (.680). Further, since the cross loadings of the items PRI5 (.697 to TR), TRI1, TRI3 and TRI4 (.643, .657 and .692 to PRI) are relatively high, the respective items were dropped in order to strengthen discriminant validity, which did not adversely affect our previously conducted analyses.

The construct's internal consistency reliability was assessed calculating the Cronbach's Alpha (CA), the inter-item correlation (IIC) and the corrected inter-scale correlation (CISC). For CA, IIC and CISC, the recommended threshold values (CA ≥ .7; IIC ≥ .3; CISC ≥ .5) are met for all constructs (see Table 2). The reliability of the constructs in terms of quality criteria of second order was assessed examining the composite reliability (CR) and the average variances extracted (AVE) (see Table 2). For both measures, the thresholds are met (CR ≥ .6; AVE ≥ .5). Regarding the indicator reliability (IR) (not listed in Table 2), the required threshold of ≥ .4 is met by all indicators (lowest IR = .545). Therefore, we assume convergent validity in the context of construct validity. Next, we evaluated the discriminant validity by checking for the Fornell-Larcker criterion, which states that the square roots of the AVE (dark cells) need to be higher than the corresponding correlations between the constructs [43]. Since this is the case for all our constructs, discriminant validity for all factors can be assumed. Thus, our constructs serve for further hypotheses testing.

Table 2. Discriminant Validity

Factor	*# Items*	*CISC*	*IIC*	*CA*	*CR*	*AVE*	*CO*	*ITU*	*PRI*	*SEC*	*TR*
CO	3	.754-.829	.752	.901	.938	.835	.914				
ITU	4	.701-.856	.708	.906	.934	.781	.578	.884			
PRI	4	.623-.683	.539	.824	.883	.653	.629	.629	.808		
SEC	5	.682-.830	.680	.914	.936	.746	.592	.607	.640	.863	
TR	4	.527-.654	.486	.791	.865	.616	.555	.580	.681	.577	.785

4.2 Hypotheses Testing

To examine the influence of the experiment conditions on the latent variables TR, CO as well as on SEC and PRI, we conducted analyses of means (two-sample t-test). To evaluate the differences between the constructs regarding cloud service (G1) and on-premise data storage (G2) before ("a" hypotheses, G1 and G2) and after a data breach ("b" hypotheses, G1E and G2E), the results of the first and the second posttest were compared between G1 and G2 (see Table 3). As the Levene tests are not significant, we assume variance homogeneity for all constructs. Since significant differences for all constructs between G1 and G2 ($p < .05$) were identified, H1a, H2a, H3a and H6a are supported. Regarding the outcome of the event on the hypotheses, no significant differences can be identified for SEC, PRI and TR except for CO ($p = .026$). Hence, except from H6b, we find support for H1b, H2b and H3b.

Table 3. Significance Levels and Mean Values

Construct	*Result*	*G1 and G2*	*G1E and G2E*
SEC	Mean Value G1; G2	3.217; .2.890	4.931; 4.850
	Sig. t-Test (Levene)	.038 (.116)	.617 (.206)
PRI	Mean Value G1; G2	2.623; 2.352	3.421; 3.188
	Sig. t-Test (Levene)	.033 (.735)	.091 (.055)
TR	Mean Value G1; G2	2.618; 2.316	3.447; 3.232
	Sig. t-Test (Levene)	.003 (.958)	.114 (.108)
CO	Mean Value G1; G2	2.798; 2.443	3.683; 3.295
	Sig. t-Test (Levene)	.029 (.506)	.026 (.388)

The relationships between the constructs and their impact on the dependent variables were evaluated using partial least squares (PLS) structural equation modeling (SEM) with SmartPLS 3.0 [44]. In order to evaluate the model fit, we checked for the CMIN/DF as well as the SRMR of the model (2.661, .073), which meet the required thresholds (CMIN/DF ≤ 3.0, SRMR ≤ .08) [45], [46]. Since further fitness criteria range slightly above or below the recommended thresholds (in brackets), i.e., CFI = .909 (≥ .9), RMSEA = .088 (≤ .08, should not exceed ≥ .1) and GFI = .837 (≥ .9), we assume a good model fit. Especially RMSEA values are debatable and thus drawing absolute cutoffs is inadvisable [41], particularly when considering smaller sample sizes with n ≤ 250 [46]. Afterwards, the path correlations of our SEM were evaluated in order to identify significant correlations between the constructs (see Figure 3).

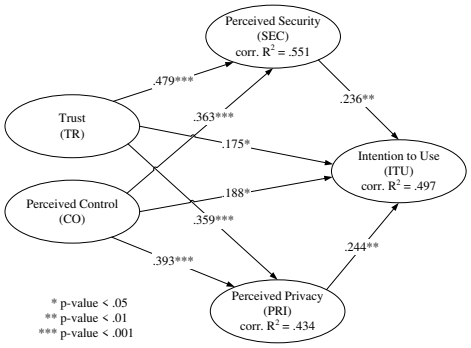

Figure 3. PLS Model

Strong statistically significant relationships between TR and SEC and PRI as well as between CO and SEC and PRI can be confirmed. Hence, we find support for H4, H5, H7 and H8 in our model. Further, path coefficients of ≥ .236 between SEC as well as PRI and ITU point to a moderate influence of both constructs on ITU. Therefore, H9 and H10 can be confirmed. Since CO and TR largely determine SEC and PRI (R^2 = .551 and .434), which again have a strong effect on the ITU and despite the relatively low but still significant ($p < .05$) path correlations (.175 and .188), we assume a low but significant impact of TR and CO on ITU. Thus, H10 and H11 can be confirmed. Based on the analyses, the statuses of our hypotheses are shown in Table 4.

Table 4. Statuses of the Hypotheses

H	*Relation*	*Status*	*H*	*Relation*	*Status*
1a	SEC(G2) > SEC(G1)	Supported	6a	CO(G2) > CO(G1)	Supported
1b	SEC(G2E) = SEC(G1E)	Supported	6b	CO(G2E) = CO(G1E)	Not Supported
2a	PRI(G2) > PRI(G1)	Supported	7	CO ↑ ⇒ SEC ↑	Supported
2b	PRI(G2E) = PRI(G1E)	Supported	8	CO ↑ ⇒ PRI ↑	Supported
3a	TR(G2) > TR(G1)	Supported	9	SEC ↑ ⇒ ITU ↑	Supported
3b	TR(G2E) = TR(G1E)	Supported	10	TR ↑ ⇒ ITU ↑	Supported
4	TR ↑ ⇒ SEC ↑	Supported	11	CO ↑ ⇒ ITU ↑	Supported
5	TR ↑ ⇒ PRI ↑	Supported	12	PRI ↑ ⇒ ITU ↑	Supported

5 Conclusion

5.1 Discussion and Implications

The results of the structural equation model indicate that TR, CO, SEC and PRI are key determinants of the intention to use PHR services. In addition, TR and CO both significantly determine SEC and PRI (H4, H5, H7, H8), which ultimately determine the ITU the provided service, independently of the underlying storage solution (cloud vs. on-premise) (H9, H10, H11, H12). Given the similar outcome of both - the storage solution and the data breach - on SEC and PRI, it is possible that the participants did not significantly differentiate between the constructs [19]. Thus, apart from the necessity to comply with strict healthcare regulations, PHR providers need to consider measures that strengthen the TR, CO and especially the SEC and PRI of potential users, e.g., by providing transparency over control, security and privacy measures. Although previous research found that the positive aspects of health clouds outweigh patients' privacy concerns [13], the results of the experiment reveal that the subjects' SEC, PRI, CO and TR are significantly higher when personal data in the form of PHRs are stored on-premise compared to cloud environments (H1a, H2a, H3a, H6a) (RQ1). Thus, despite the relatively high maturity of the technology and the efforts undertaken by theory and practice, CC still faces skepticism regarding the provisioning of PHRs. Providers of PHR solutions need to be aware of this perception and have to decide whether to offer their services via cloud environments or on-premise solutions. When offering cloud-based PHR services, providers might rely on private clouds in order to minimize concerns on the users' side. Further, hybrid cloud infrastructures can be used for encrypted or non-sensitive data in order to realize cloud-related benefits. However, in case of a data breach, no significant differences regarding SEC, PRI and TR between the two solutions could be determined (H1b, H2b, H3b), except for CO (H6b) (RQ2). In cloud environments, data breaches might entail a considerably larger impact on the side of the provider compared to on-premise environments [23]. Hence, cloud services need to emphasize their measures regarding security and privacy and foster the trust of (potential) end-users, e.g., by providing certifications [8], as cloud users seek for external control agents [11]. In order to

avoid severe consequences for PHR service users in case of a data breach, strong encryption mechanisms should be implemented [1], [15]. Although both storage solutions were compliant to ISO27001, the SEC, PRI and TR in the cloud scenario were found to be lower. Thus, besides providing certifications, further measures are necessary in order to foster users' perceptions of the constructs. In addition, the experiment revealed that the participants' CO regarding the on-premise solution is still significantly higher after a data breach, even though the participants' abilities regarding control did not vary between the experiment groups. This is presumed to be ascribed to the control delegation and the associated reservations towards cloud environments, which draws the attention of cloud-based PHR providers on establishing measures to particularly foster their users' CO.

5.2 Limitations and Future Research

Since the applied vignette technique puts the participants in a fictitious scenario, the behavior of the subjects might be different compared to a real-world scenario [35]. In addition, using students as experiment participants is not without controversy in the field of information systems and partially limits the generalizability of the results. However, since students reflect the future target group and are early adopters of innovative technologies, such as CC and PHRs, we argue that students are an adequate sample group for the experiment conducted [24], [32]. In this context, it is necessary to note that the experiment was conducted based on a relatively homogeneous sample group, which might influence the overall results. Concerning the evaluation of the model fit, our research model revealed slight weaknesses in terms of some fit indices. Nevertheless, since the deviations from the recommended thresholds are relatively small and cutoff thresholds are discussed controversially [41], we argue that the overall model is not endangered. Further, although established items for measuring trust were derived from the literature [37], several items had to be dropped. Yet, since we used reflective measurement, the meaning of the constructs TR, PRI and SEC was not affected [39], [40]. However, using constructs which strongly differ in the number of items (e.g., TR and ITU) might lead to distorted results. In addition, due to the temporal proximity of the two posttests conducted, an impact of the first on the second survey resulting in a certain bias is possible.

Regarding the data breach, the manipulation of the subjects can possibly be ascribed to multiple factors. In G1, the data are stored externally at a cloud provider, whereas in G2, the data are stored on-premise, which might lead to different accusations towards the actors. However, the examined scenarios reflect the practical problem of companies whether to provide their services via external cloud solutions or on-premise data centers [8], [17]. In this context, it needs to be noted that the use of certain PHR systems might not be purely voluntarily, but instead stipulated by politics or certain healthcare actors. Although control is seen as a core principle of privacy [30], the adoption of privacy as control in the course of this study can be regarded as simplification of the complex nature of the construct [22], [30]. As we concentrated on trust and control as influencing factors of SEC and PRI, the examination of further constructs or the application of behavioral explanation models is possible.

Our study provides multiple starting points for future work. For example, besides investigating TR and CO as influencing factors of PRI and SEC, further constructs (e.g., benefits) can be examined regarding their influence on the two constructs. Additionally, the cause for the higher perceived control in the on-premise solution after a data breach and the correspondingly adjusted levels of SEC, PRI and TR allow for further investigation. A practical validation of the results by means of an examination of a commercial PHR provider, e.g., in the form of a case study, is desirable. In this context, the implications and results from the present study may serve as a foundation for additional qualitative studies or the examination of actual privacy behaviors. Moreover, our experimental setup even allows for richer insights and analyses, e.g., a cross-comparison between the groups before and after the breach.

6 Acknowledgements

The authors would like to thank the experiment participants, the other project members, specifically Ms. Miftari and Ms. Imhorst, for their valuable and substantive help, as well as the reviewers for their constructive feedback. This contribution was prepared within the research project "Dorfgemeinschaft 2.0". The project is funded by the Federal Ministry for Education and Research (BMBF) (funding code 16SV7453).

References

1. Kaletsch, A., Sunyaev, A.: Privacy Engineering: Personal Health Records in Cloud Computing Environments. In: Proceedings of the 32nd International Conference on Information Systems. Shanghai, China (2011).
2. Menachemi, N., Collum, T.H.: Benefits and Drawbacks of Electronic Health Record Systems. Risk Management and Healthcare Policy. 4, 47–55 (2011).
3. Kuo, A.M.-H.: Opportunities and Challenges of Cloud Computing to Improve Health Care Services. Journal of Medical Internet Research. 13 (2011).
4. Zissis, D., Lekkas, D.: Addressing Cloud Computing Security Issues. Future Generation Computer Systems. 28, 583–592 (2012).
5. Li, M., Yu, S., Zheng, Y., Ren, K., Lou, W.: Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Transactions on Parallel and Distributed Systems. 24, 131–143 (2013).
6. Muhammed, I., Wickramasinghe, N.: User Perceptions and Expectations of the Personally Controlled Electronic Health Record (PCEHR): A Case Study of Australia's e-Health Solution. In: Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 3441–3450. HI, USA (2017).
7. Angst, C.M., Agarwal, R.: Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. MIS Quarterly. 33, 339–370 (2009).
8. Rodrigues, J.J.P.C., De La Torre, I., Fernández, G., López-Coronado, M.: Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems. Journal of Medical Internet Research. 15 (2013).
9. Tschirsich, M., Schröder, T.: Schwachstellen in Gesundheits-App Vivy, https://www.modzero.ch/static/vivy-app-security-final.pdf (Accessed: 20.11.2018)

10. Wikina, S.B.: What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches. Perspectives in Health Information Management. 11, (2014).
11. Lang, M., Wiesche, M., Krcmar, H.: Perceived Control and Privacy in a Professional Cloud Environment. In: Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 3668–3677. HI, USA (2018).
12. Fishbein, M., Ayzen, I.: Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Addison-Wesley, Reading (1975).
13. Ermakova, T., Fabian, B., Zarnekow, R.: Acceptance of Health Clouds - a Privacy Calculus Perspective. In: Proceedings of the 22nd European Conference on Information Systems. Tel Aviv, Israel (2014).
14. Plachkinova, M., Alluhaidan, A., Chatterjee, S.: Health Records on the Cloud: A Security Framework. In: International Conference on Health Informatics and Medical Systems, pp. 152–158. Las Vegas, NV, USA (2015).
15. Li, M., Yu, S., Ren, K., Lou, W.: Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings. In: International Conference on Security and Privacy in Communication Systems, pp. 89–106. Singapore (2010).
16. Arpaci, I., Kilicer, K., Bardakci, S.: Effects of Security and Privacy Concerns on Educational Use of Cloud Services. Computers in Human Behavior. 45, 93–98 (2015).
17. Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A.: Security and Privacy in Electronic Health Records: A Systematic Literature Review. Journal of Biomedical Informatics. 46, 541–562 (2013).
18. Ermakova, T., Fabian, B., Zarnekow, R.: Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios. In: Proceedings of the 19th Americas Conference on Information Systems. Chicago, IL, USA (2013).
19. Crossler, R.E., Bélanger, F.: The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors. In: Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 4071–4080. HI, USA (2017).
20. Flavián, C., Guinalíu, M.: Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Website. Industrial Management & Data Systems. 106, 601–620 (2006).
21. Norberg P.A., Horne, D.R., Horne, D.A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. The Journal of Consumer Affairs. 41, 100–126 (2007).
22. Crabtree, A., Tolmie, P., Knight, W.: Repacking 'Privacy' for a Networked World. Computer Supported Cooperative Work: CSCW: An International Journal. 26, 453–488 (2017).
23. Grobauer, B., Walloschek, T., Stöcker, E.: Understanding Cloud Computing Vulnerabilities. IEEE Security and Privacy. 9, 50–57 (2011).
24. Adelmeyer, M., Walterbusch, M., Biermanski, P., Teuteberg, F.: Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems. In: Proceedings of the 26th European Conference on Information Systems. Portsmouth, UK (2018).
25. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management Review. 20, 709–734 (1995).
26. Söllner, M., Hoffmann, A., Leimeister, J.M.: Why Different Trust Relationships Matter for Information Systems Users. European Journal of Information Systems. 25, 274–287 (2016).

27. Walterbusch, M., Martens, B., Teuteberg, F.: Exploring Trust in Cloud Computing: A Multi-Method Approach. In: Proceedings of the 21st European Conference on Information Systems (ECIS 2013). Utrecht, Netherlands (2013).
28. Mitchell, V.-W.: Consumer Perceived Risk: Conceptualisations and Models. European Journal of Marketing. 33, 163–195 (1999).
29. Hsin Chang, H., Wen Chen, S.: The Impact of Online Store Environment Cues on Purchase Intention: Trust and Perceived Risk as a Mediator. Online Information Review. 32, 818–841 (2008).
30. Acquisti, A., Brandimarte, L., Lowenstein, G.: Privacy and Human Behavior in the Age of Information. Science. 347, 509–514 (2015).
31. Lee, Y.E., Benbasat, I.: The Influence of Trade-off Difficulty Caused by Preference Elicitation Methods on User Acceptance of Recommendation Agents across Loss and Gain Conditions. Information Systems Research. 22, 867–884 (2011).
32. Walter, N., Öksüz, A., Walterbusch, M., Teuteberg, F., Becker, J.: "May I help You?" Increasing Trust in Cloud Computing Providers through Social Presence and the Reduction of Information Overload. In: Proceedings of the 35th International Conference on Information Systems. Auckland, NZ (2014).
33. Mathieson, K.: Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. Information Systems Research. 2, 173–191 (1991).
34. Pavlou, P.A., Fygenson, M.: Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. MIS Quarterly. 30, 115–143 (2006).
35. Aguinis, H., Bradley, K.J.: Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. Organizational Research Methods. 17, 351–371 (2014).
36. Shadish, W.R., Cook, T.D., Campbell, D.T.: Experimental and Quasi-Experimental Designs for Generalized Causal Inference. Houghton Mifflin, Boston, NY (2002).
37. McKnight, D.H., Choudhury, V., Kacmar, C.: Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. Information Systems Research. 13, 334–359 (2002).
38. Podsakoff, P.M., Organ, D.W.: Self-Reports in Organizational Research: Problems and Prospects. Journal of Management. 12, 531–544 (1986).
39. Burns, R.P., Burns, R.: Business Research Methods and Statistics using SPSS. Sage, London (2008).
40. Jarvis, C.B., MacKenzie, S.B., Podsakoff, P.M.: A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. Journal of Consumer Research. 30, 199–218 (2003).
41. Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E.: Multivariate Data Analysis. Pearson, Harlow, GB (2014).
42. Nunnally, J.C., Bernstein, I.H.: Psychometric Theory. McGraw-Hill, New York, NY, USA (1994).
43. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research. 18, 39–50 (1981).
44. Ringle, C.M., Wende, S., Becker, J.: SmartPLS 3, http://www.smartpls.com. (2015).
45. Hornburg, C., Giering, A.: Konzeptualisierung und Operationalisierung komplexer Konstrukte. Ein Leitfaden für die Marketingforschung. Marketing ZfP. 18, 5–24 (1996).
46. Hu, L., Bentler, P.M.: Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives. Structural Equation Modeling: A Multidisciplinary Journal. 6, 1–55 (1999).