Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2014 Proceedings

ACCEPTANCE OF HEALTH CLOUDS - A PRIVACY CALCULUS PERSPECTIVE

Tatiana Ermakova
Technical University of Berlin, Berlin, Germany, tatiana.ermakova@tu-berlin.de

Benjamin Fabian
Humboldt-Universität zu Berlin, Berlin, Germany, bfabian@wiwi.hu-berlin.de

Rüdiger Zarnekow
Technical University of Berlin, Berlin, Germany, ruediger.zarnekow@tu-berlin.de

Tatiana Ermakova, Benjamin Fabian, and Rüdiger Zarnekow, 2014, "ACCEPTANCE OF HEALTH CLOUDS - A PRIVACY CALCULUS PERSPECTIVE", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0
http://aisel.aisnet.org/ecis2014/proceedings/track09/11

ACCEPTANCE OF HEALTH CLOUDS – A PRIVACY CALCULUS PERSPECTIVE

Complete Research

Ermakova, Tatiana, Technical University of Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, tatiana.ermakova@tu-berlin.de

Fabian, Benjamin, Humboldt-Universität zu Berlin, Spandauer Straße 1, 10178 Berlin, Germany, bfabian@wiwi.hu-berlin.de

Zarnekow, Rüdiger, Technical University of Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, ruediger.zarnekow@ikm.tu-berlin.de

Abstract

The cloud computing paradigm promises to significantly improve the transfer of crucial medical records during medical service delivery. However, since cloud computing technology is still known for unsolved security and privacy challenges, severe concerns could prevent patients and medical workers from accepting such an application scenario. Owing to the lack of similar studies, we investigate what determines an individual's information privacy concerns on cloud-based transmission of medical records and whether perceived benefits influence the behavioral intention of individuals to permit medical workers to transfer their medical records via cloud-based services. Based on different established theories, we develop and empirically test a corresponding research model by a survey with more than 260 full responses.

Our results show the perceived benefits of this health cloud scenario override the impact of information privacy concerns even in the privacy-sensitive German-speaking area and immediately after the NSA scandal. Somewhat surprisingly, we also find that in this scenario knowledge about information privacy has no significant effect on information privacy concerns although some relations have been observed in previous empirical studies. Finally, patient information privacy concerns can be mitigated by establishing trust in cloud providers in healthcare as well as in privacy-preserving technological and regulatory mechanisms.

Keywords: Cloud Computing, Healthcare, Privacy, Behavioral Intention, Structural Equation Modeling.

1 Introduction

The cloud computing paradigm, which enables on-demand access to a network-based cluster of shared computing and storage resources (e.g., Mell and Grance, 2012), promises to significantly improve the transfer of medical records, which is crucial during the service delivery by medical workers (Karthikeyan and Sukanesh 2012; Poulymenopoulou et al. 2011). Current procedures for medical records transmission usually produce long waiting times, resulting in the delay of treatment-related decisions or repetitive medical diagnostics. Using a cloud-based system, medical records could be encrypted and sent from a current medical institution (a hospital or a doctor) to another one just in the right moment. We will further refer to the application scenario as health cloud scenario.

Despite a relatively high general popularity of cloud computing with end users, this technology still raises wide concerns among them (Ion et al., 2011), in particular among patients and medical workers (Deng et al., 2012) due to still unsolved security and privacy challenges. This may slow down or impede acceptance of the apparently beneficial application of clouds in healthcare.

Owing to the lack of similar studies and aiming to support the TRESOR (TRusted Ecosystem for Standardized and Open cloud-based Resources) research project (TRESOR, 2014), we address the privacy calculus perspective in individuals' behavioral intention to accept the health cloud scenario and permit medical workers to transfer their medical records via a cloud-based service. The privacy calculus theory states that individuals are willing to reveal private information about them in exchange for certain benefits (e.g., Dinev and Hart, 2006; Smith et al., 2011). Among other theories applied to interpret the establishment of information privacy concerns and their consequences, for example as summarized by Li (2011), it reflects the cost-benefit analysis an individual is supposed to face in the age of the digitalization of healthcare industry (Dinev et al., 2012).

We conduct our research following the structural equation modelling (SEM) research guidelines by Urbach and Ahlemann (2010), MacKenzie et al. (2011), Petter et al. (2007), Gefen et al. (2000) and Chin (1998), formulating our research questions as follows: (1) Which determinants are responsible for explaining the variation in the extent to which individuals are concerned about their information privacy in the health cloud scenario? (1a) How does the knowledge about information privacy (both stated and actual) influence the individuals' concerns for the privacy of patient information? (1b) How does the trust in privacy-preserving regulatory and technological mechanisms and in cloud provider(s) in healthcare influence the individuals' concerns for the privacy of patient information? (2) Are information privacy concerns dominated by the perceived benefits of cloud-based transmission of medical data in influencing the behavioral intention to accept the health cloud scenario?

Based on recent privacy research in general (Pavlou, 2011; Smith et al., 2011; Belanger and Crossler, 2011) and in the healthcare context (Dinev et al., 2012; Angst and Agarwal, 2009; Bansal et al., 2010; Laric et al., 2009; Rohm and Milne, 2004) and the unified theory of acceptance and use of technology (Venkatesh et al., 2003; Venkatesh et al., 2012), we deduce the determinants of both the behavioral intention to accept the health cloud scenario and patient information privacy concerns and hypothesize the relations in a causal model. Then we operationalize each of the model's constructs with a set of measurement items in reflective mode. Accordingly, we developed a questionnaire and pre-tested it with multiple responders of different age, gender and education. Next, we collected empirical data and performed data analysis using the partial least squares (PLS) approach. To answer the research questions, we tested the structural equation model. Finally, we summarize the results and findings, before we derive suggestions for future research and the implications for theory and practice and present conclusions.

2 Theoretical Foundations

In information systems (IS) research, UTAUT (Venkatesh et al., 2003) represents a synthesis of eight models specifying the factors that lead an individual to accept or reject a technology. UTAUT was found to outperform each of these single models with R^2 of 68 percent. Along with UTAUT2 (Venkatesh et al., 2012), UTAUT offers a conceptual lens for investigating individuals' acceptance.

Further we base our research on the information privacy research summarized by Li (2011), Belanger and Crossler (2011), Smith et al. (2011), and Pavlou (2011). The works provide a review on previous empirical studies in this area, and discuss antecedents and consequences of information privacy concerns.

Though there are multiple theories interpreting the formation of information privacy concerns and their consequences, for example those summarized by Li (2011), we adopt the privacy calculus theory as overarching framework in our research study, as the privacy calculus theory addresses the cost-benefit perspective explaining individuals' decisions in the age of the digitalization of healthcare industry (Dinev et al., 2012). According to this theory, individuals seek to obtain certain benefits when revealing private information about them (e.g., Dinev and Hart, 2006; Smith et al., 2011; Pavlou, 2011). Dinev et al. (2012) investigate individuals' attitudes towards electronic health records from a privacy calculus perspective and, among other results, show that privacy calculus components, such as health information privacy concerns, perceived benefits and convenience, significantly compete in influencing attitudes towards electronic health records (EHRs). Further empirical studies examining patients' information privacy concerns can be found in the works by Angst and Agarwal (2009), Bansal et al. (2010), Laric et al. (2009), and Rohm and Milne (2004). Our work extends earlier approaches and investigates the acceptance of transmitting medical data such as EHRs through Cloud Computing.

2.1 Patient Information Privacy Concerns

Due to the global and open nature of the Internet, personal information can be easily collected, stored, and capitalized by multiple parties. Firms collect customer information through their websites in order to utilize it for customized advertising (Pavlou, 2011), or share it with affiliated companies (Smith et al., 2011). In healthcare, Kaletsch and Sunyaev (2011) also observe these practices among firms that are processing and providing personal health records (PHRs). Due to this provisioning and sharing of user data with other parties, confidential data can be lost or stolen (Smith et al., 2011). In the case of unwanted or unwarranted disclosure and exchange of sensitive personal health information, patients may experience situations ranging from unsolicited direct mailings from medical products or service marketers (Rohm and Milne, 2004) to impaired employment opportunities (Bansal et al., 2010; Laric et al., 2009; Rohm and Milne, 2004) as well as damage to social acceptance and individual relationships (Rohm and Milne, 2004; Laric et al., 2009).

There are multiple definitions of information privacy provided in the literature that try to conceptualize the resulting concerns (Pavlou, 2011; Belanger and Crossler, 2011; Smith et al., 2011). Belanger and Crossler (2011) define information privacy as a merge of personal communication and data privacy, which, along with privacy of a person and behavior privacy, build the four distinct dimensions of privacy, while in the IS discipline context Smith et al. (2011) conceptualize information privacy as one's control over personal information.

In general, empirical studies conclude that information privacy concerns have a negative impact on the willingness to provide information for transaction (Li, 2011). The results of the study by Rohm and Milne (2004) indicate that consumers are most concerned with the collection and use of personal medical information, in contrast to other types of information typically collected by direct marketers. In the healthcare context, information privacy concerns have also been shown to exert a negative impact on the likelihood of individuals accepting EHRs (Angst and Agarwal, 2009), their attitude toward EHRs (Dinev et al., 2012), and their intention to disclose healthcare information to health websites (Bansal et al., 2010). Therefore, we hypothesize that:

Hypothesis 1. Patient information privacy concerns will be negatively associated with behavioral intention to accept the health cloud scenario.

To operationalize patient information privacy concerns, we apply the scales developed by Smith et al. (1996), which include collection, errors, unauthorized secondary use, and improper access to information. These dimensions were revalidated in the healthcare context by Dinev et al. (2012) and are commonly regarded as some of the most reliable scales (Smith et al., 2011).

2.2 Trust in Privacy-Preserving Regulatory and Technological Mechanisms, and in Cloud Providers in the Healthcare Sector

Trust beliefs reflect the extent to which people believe an object of their trust is dependable in protecting their personal information. Trust beliefs have been shown to have a significant impact on information privacy concerns (Li, 2011). Li (2011) further observes that multiple studies confirm the mitigating role of more restrictive government regulations on information privacy concerns. Dinev et al. (2012) find that perceived effectiveness of privacy-preserving technological and regulatory mechanisms involves a positive effect on trust in EHR and a reduction of information privacy concerns. Similar to the study by Dinev et al. (2012) and other studies surveyed by Li (2011) and Smith et al. (2011), we suggest trust in privacy-preserving technological and regulatory mechanisms to be an antecedent to information privacy concerns and state that:

Hypothesis 2. Trust in privacy-preserving technological mechanisms will be negatively associated with patient information privacy concerns.

Hypothesis 3. Trust in privacy-preserving regulatory mechanisms will be negatively associated with patient information privacy concerns.

The results of the study by Rohm and Milne (2004) indicate a low level of trust among consumers with respect to organizations collecting, using, and sharing their personal medical information. Furthermore, the authors show that the lower the level of trust in those organizations is, the greater the concerns for information privacy are. Therefore, we postulate that:

Hypothesis 4. Trust in cloud provider(s) in the healthcare sector will be negatively associated with patient information privacy concerns.

2.3 Privacy Awareness: Stated vs. Actual

Privacy awareness refers to the degree to which an individual is informed about privacy issues. The construct implies that individuals who are not aware about privacy issues will probably not be concerned about them while using the health cloud scenario. Li (2011) observes that a person's knowledge is closely related to her or his level of information privacy concerns and differentiates between general knowledge about Internet use and specific knowledge about privacy invasions. Li (2011) states the impact of specific knowledge on information privacy concerns is consistently shown to be positive, whereas empirical evidences of the impact of general knowledge on information privacy concerns provide mixed results. Li (2011) further suggests these could be explained by the variety of Internet knowledge and the possible non-linearity of the relationship between general knowledge and information privacy concerns: "*as the knowledge of privacy issues grows, a person may become more concerned about online privacy; with further accumulation of knowledge, the person may learn to avoid some of the privacy risks and therefore become less concerned*".

Brecht et al. (2012) apply this differentiation in their research and find a negative correlation between stated and actual privacy literacy in the context of communication anonymizers, thus showing that an individual's self-assessment may not reflect the actual degree of her or his knowledge about online privacy risks. Therefore, we also measure both stated and actual privacy awareness and hypothesize that:

Hypothesis 5. Stated privacy awareness will be positively associated with patient information privacy concerns.

Hypothesis 6. Actual privacy awareness will be positively associated with patient information privacy concerns.

2.4 Perceived Benefits of Cloud-Based Data Transmission

In the context of the present study, the perceived benefits of cloud-based data transmission are understood as the expected relative advantages associated with the usage of the health cloud scenario such as the ability to reckon on the timely delivery of medical records to medical offices when they are needed and the fast provision of medical services, to eliminate unnecessary travel to and from medical offices and to avoid repetitive medical diagnostics.

Hypothesis 7. Perceived benefits of the health cloud scenario will be positively associated with behavioral intention to accept it.

2.5 Control Variables

Demographic factors such as age and gender may have an impact on information privacy concerns (Li, 2011). The results of the study by Laric et al. (2009) demonstrate that females generally rank their concerns for health information privacy higher than males. Laric et al. (2009) also find significantly higher mean concerns for the privacy of health information privacy among subjects in the 45 and over age category as compared to younger subjects.

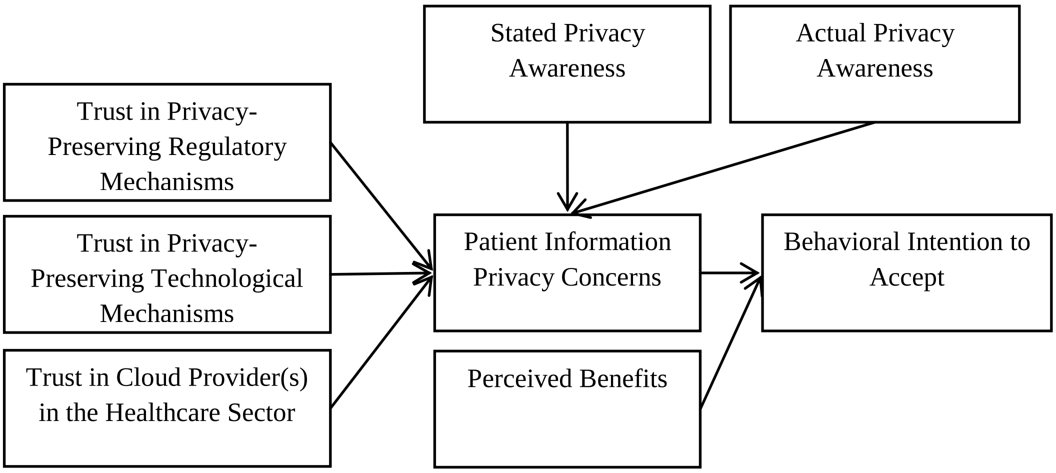
Stated Privacy Awareness
Actual Privacy Awareness
Trust in Privacy-Preserving Regulatory Mechanisms
Trust in Privacy-Preserving Technological Mechanisms
Trust in Cloud Provider(s) in the Healthcare Sector
Patient Information Privacy Concerns
Perceived Benefits
Behavioral Intention to Accept

Figure 1. Research Model.

The study by Bansal et al. (2010) shows a positive indirect impact of poor health status on health information privacy concerns. Laric et al. (2009) observe significantly higher mean concerns for health information privacy under more severe, sensitive, or contagious health conditions. Laric et al. (2009) relate the study results to the fact that older people suffer from more ailments or conditions, whereas Bansal et al. (2010) suggest less healthy individuals are more concerned with respect to their personal health information as its disclosure could damage their status, employment opportunities, or social standing. Bansal and Davenport (2010) investigate the moderating role of perceived health status on privacy concern factors and intentions to transact with highly versus lowly trustworthy health websites and find the support of these hypotheses related to collection, error related, and secondary use; interestingly, the last one with negative impact.

It is considered out of the scope of this paper to formally test the direct impact of age and gender on any of the constructs in our research model. We therefore operationalize these factors along with personal health condition as control variables to illuminate the variance explained by them.

3 Model Construction and Instrument Development

Our hypothesized model drawn from the theoretical foundations in section 2 is presented in Figure 1 and includes eight constructs. Two of them, namely patient information privacy concerns and the perceived benefits of the health cloud scenario, are hypothesized to be significant direct determinants of individuals' behavioral intention to accept the health cloud scenario. The remaining constructs, including the trust in privacy-preserving regulatory and technological mechanisms, cloud provider(s), in the healthcare sector appear to indirectly influence it.

Construct	**Item**
Behavioral Intention to accept the Health Cloud Scenario (BI)	Imagine, that your sensitive patient data could be encrypted and sent from your current medical institution to another (a hospital or a doctor) just in the right moment using a cloud-based system. Given the above mentioned circumstances, how likely would you approve to the transmission if … … your patient data could otherwise arrive not in time. … it is an emergency situation. … your patient data could otherwise be transferred via fax. … your patient data could otherwise be transferred via taxi. … you would have to deal with the transmission yourself. … the part of your patient data you consider to be sensitive is not transferred. … your patient data is pseudonymized before being encrypted.
Perceived Benefits of the Health Cloud Scenario (PB)	To what extent would you agree with these statements? I find that the benefits of the above described application scenario override my concerns of possible information privacy risks. The greater the benefits from the application scenario, the more I tend to suppress my information privacy concerns. In general, my need to use the application scenario is greater than my concern about information privacy. (Adapted from Dinev and Hart (2006))
Patient Information Privacy Concerns – Improper Access (CA)	To what extent would you be concerned that … … unauthorized people can access your patient data in the cloud. … your patient data is not enough protected against unauthorized access. … that unauthorized access to your patient data can hardly be prevented. … that unauthorized access to your patient data can hardly be detected.
Patient Information Privacy Concerns – Errors (CE)	To what extent would you be concerned that … … your patient data can be modified by unauthorized people. … your patient data are not enough protected against modifications by unauthorized people. … unwanted modifications to your patient data by unauthorized people can hardly be prevented. … unwanted modifications to your patient data by unauthorized people can hardly be detected. … your patient data are delivered not substantially correct to the recipient. … your patient data are delivered not timely to the recipient.
Patient Information Privacy Concerns – Collection (CC)	To what extent would you be concerned that your patient data in the cloud … … doesn't get deleted from the cloud after the recipient received them. … are kept as a copy after the recipient received them. … are collected by the cloud provider after the recipient received them.

Table 2. Research Model Constructs and Related Questionnaire Items (Part 1).

In Table 2, we present the measurement items of the survey instrument. It should be noted that for measuring actual privacy awareness we use one item reflecting the score obtained by answering the presented questions. For validation purposes, we conducted some pre-tests and a pilot study with multiple responders of different age, gender and education. In general, they resulted in only minor changes to the initial instrument.

Construct	**Item**
Patient Information Privacy Concerns – Unauthorized Secondary Use (CU)	To what extent would you be concerned that your patient data in the cloud can be … … found by someone unintended. … manipulated by someone unintended. … used in a way you did not foresee. … misused by someone unintended. … made available to companies or unknown parties without your knowledge. … sold to companies or unknown parties. … used for commercial purposes. … continuously spied on. (Adapted from Dinev and Hart (2006), Krasnova et al. (2010))
Trust in Privacy-Preserving Regulatory Mechanisms (TR)	To what extent would you agree that the current regulatory mechanisms … … protect your patient data in the cloud against misuse. … reliably govern the practice of how your patient data in the cloud is protected, collected and distributed. … are enough to counteract the misuse of your patient data. (Inspired by Dinev et al. (2012))
Trust in Privacy-Preserving Technological Mechanisms (TT)	To what extent would you agree that the current technological mechanisms … … can effectively protect against unauthorized access and modifications to your patient data in the cloud. … can reliably implement the regulations of how your patient data in the cloud is to be protected, collected and distributed. … are enough to counteract unauthorized access and modifications to your patient data.
Trust in Cloud Provider(s) in the Healthcare Sector (TC)	To what extent would you agree that the content and storage provider working for the health sector … … can reliably implement the regulations of how your patient data in the cloud is to be protected, collected and distributed. … are trustworthy. …act in good faith.
Stated Privacy Awareness (SA)	To what extent would you agree with these statements? I am aware of the information privacy risks and preserving mechanisms. I follow the news and developments about the information privacy risks and preserving mechanisms. I keep myself updated about information privacy risks and possible solutions to ensure my information privacy. (Adapted from Xu et al. (2011))
Gender	May we ask about your gender? Male. Female.
Age	May we ask, how old are you? < or equal 20 Years. 21 – 30 Years. 31 – 40 Years. 41 – 50 Years. 51 – 60 Years. 61 – 70 Years. > 70 Years.
Health Status	How would you say your current health status in general is? Very Good. Good. Rather Good. Neither Good Nor Poor. Rather Poor. Poor. Very Poor.

Table 2. Research Model Constructs and Related Questionnaire Items (Part 2).

4 Data Collection

We collected the responses to our online survey in November and December 2013. We sent invitations to the survey via numerous mailing lists as well personally addressed people in our personal networks to participate in the survey and also to invite further people in their networks. As rewards for time and effort we had a prize draw of 10 Amazon vouchers worth 10 EUR and 5 Amazon vouchers worth 20 EUR among all participants with complete questionnaires. As the study was based mainly in Germany and Switzerland, the majority of the participants were either German or Swiss or foreigners living in these countries.

Construct	Item
Actual Privacy Awareness (AW)	Can your Webmail provider see and modify the documents you have in attachments in your email account? a) They can neither look at nor modify any of my documents. b) They can see them, but not modify them. c) They can possibly see and modify them. d) I don't know. (Solution: c) When you delete a file attached to an email in your Webmail account, what do you think happens? a) The file gets permanently deleted just as when I would delete it from my computer. b) Some copies might still exist, but only for a few weeks or possibly longer, until the company manages to delete all of them. c) I don't know. (Solution: b) (Inspired by Ion et al. (2011)) Which of the following protocols can provide confidentiality for e-mail transmission? (Only one answer is correct.) a) Sec4Mail. b) POPSEC. c) PGP. d) SIMAP. e) I don't know. (Solution: c) How can a Web site distinguish its users from another? (Multiple answers could be correct.) a) Login name. b) IP address. c) Cookie. d) Browser Version and Configuration. e) I don't know. (Solution: a, b, c, d) Which of the following statements are true? a) When you are surfing the Web without encryption, your Internet provider can observe the content of the Web site you are surfing to. b) When you are surfing the Web using encryption, your Internet provider can observe the content of the Web site you are surfing to. c) When you are surfing the Web using encryption, the Web server can observe the content of the Web site you are surfing to. d) When you are surfing the Web without encryption, any router on the way to the server can observe the content of the Web site you are surfing to. e) I don't know. (Solution: a, c, d) Which of the following protocols are used during Web surfing? (Multiple answers could be correct.) a) HTTP. b) IMAP. c) TCP. d) IP. e) I don't know. (Solution: a, c, d) Which of the following actions may enhance your privacy while surfing the Web? (Multiple answers could be correct.) a) Use of a Web proxy. b) Always accepting cookies. c) Deleting the browser history. d) Not revealing your personal data. e) I don't know. (Solution: a, c, d) What are Web proxies useful for? (Multiple answers could be correct.) a) To hide the IP address of a computer. b) To speed up access to Web sites (using caching). c) To block undesired Web sites. d) To hide the location of a computer. e) I don't know. (Solution: a, b, c, d) (Brecht et al., 2012)

Table 2. Research Model Constructs and Related Questionnaire Items (Part 3).

Gender			**Age**			**Health Status**		
Female	141	53.01%	< = 20 Years	28	10.53%	Very Good	67	25.19%
Male	120	45.11%	21 – 30 Years	175	65.79%	Good	128	48.12%
Unknown	5	1.88%	31 – 40 Years	44	16.54%	Rather Good	43	16.17%
			41 – 50 Years	4	1.50%	Neither Nor	9	3.38%
			51 – 60 Years	10	3.76%	Rather Poor	10	3.76%
			61 – 70 Years	0	0.00%	Poor	3	1.13%
			> 70 Years	2	0.75%	Very Poor	1	0.38%
			Unknown	2	0.75%	Unknown	5	1.88%

Table 3. Respondent Demographics and Health Status.

Before starting the online survey, participants were encouraged to learn more about the notion of cloud computing by following a link where a short definition adopted from a study book on introduction to information systems (Laudon et al., 2010, p. 218, in German) was presented. Cloud computing was explained as describing the possibility to request software services or data over the Internet (e.g., Google Docs).

The final net sample consisted of 266 observations. Slightly more than half of the participants (53.01%) were females, 45.11% reported to be males (see Table 3). The majority of the responders (65.79%) were aged between 21 and 30 years old, while 16.54% reported to be between 31 and 40 years old and 10.53% were in the youngest age interval of under 20. 48.12%, 25.19% and 16.17% of the respondents reported their health as good, very good and rather good, respectively.

5 Model Testing

Following the recommendations by Gefen et al. (2000), we first assess the quality of our measures by applying confirmatory factor analysis (CFA) and then test our hypotheses by using the Structural Equation Modeling's (SEM) Partial Least Square (PLS) method in SmartPLS 2.0 (Ringle et al., 2005). Similar to many other previous empirical studies (e.g., Dinev et al., 2012; Xu et al., 2011), we chose PLS for testing as the method is accepted as well suitable in the presence of a large number of constructs and relationships (Chin, 1998).

It should be noted that we analyse patient information privacy concerns (C) as a second-order latent variable which we construct of the related first-order variables, i.e., improper access (CA), errors (CE), collection (CC), unauthorized secondary use (CU) (Wetzels et al., 2009).

We first controlled for gender, age and health status with respect to information privacy concerns. Since none of them had significant effect, we omitted them from further discussion.

5.1 Measurement Model

We evaluate the measurement model by examining the convergent validity and discriminant validity of the research instrument. Convergent validity refers to the degree to which measures of the same construct agree, whereas discriminant validity shows the degree to which measures of different constructs are distinct (e.g., Urbach and Ahlemann, 2010; Xu et al., 2011).

	AA	BI	PB	C	TR	TT	TC	SA
AA	1.00	-0.10	-0.17	0.07	-0.05	0.09	-0.01	0.31
BI	-0.14	0.85	0.67	-0.41	0.34	0.26	0.35	0.01
	-0.11	0.78	0.59	-0.26	0.30	0.20	0.32	0.07
	-0.02	0.81	0.65	-0.42	0.27	0.29	0.27	0.04
	-0.03	0.84	0.64	-0.44	0.26	0.24	0.35	0.04
	-0.12	0.82	0.65	-0.44	0.28	0.27	0.28	0.00
	-0.05	0.82	0.59	-0.37	0.23	0.26	0.32	0.13
	-0.10	0.78	0.61	-0.36	0.31	0.27	0.32	0.07
PB	-0.14	0.67	0.92	-0.41	0.40	0.32	0.40	-0.02
	-0.16	0.76	0.94	-0.51	0.38	0.34	0.42	-0.07
CU	0.07	-0.42	-0.46	0.94	-0.43	-0.40	-0.46	0.11
CA	0.11	-0.49	-0.52	0.86	-0.39	-0.39	-0.43	0.15
CC	0.10	-0.39	-0.43	0.68	-0.35	-0.37	-0.47	0.07
CE	-0.02	-0.31	-0.28	0.80	-0.23	-0.27	-0.33	0.06

Table 4. Item Loadings and Cross-Loadings (Part 1).

	AA	BI	PB	C	TR	TT	TC	SA
TR	-0.02	0.33	0.39	-0.39	0.93	0.49	0.45	-0.01
	-0.06	0.33	0.38	-0.39	0.93	0.48	0.44	-0.03
	-0.05	0.31	0.39	-0.40	0.90	0.48	0.46	-0.10
TT	0.08	0.29	0.35	-0.39	0.49	0.95	0.38	-0.01
	0.06	0.30	0.32	-0.40	0.47	0.92	0.44	-0.05
	0.09	0.29	0.34	-0.40	0.50	0.92	0.42	-0.06
TC	-0.03	0.36	0.43	-0.46	0.53	0.53	0.81	-0.11
	-0.03	0.34	0.40	-0.41	0.41	0.36	0.90	0.02
	0.04	0.23	0.22	-0.33	0.20	0.15	0.74	0.12
SA	0.24	0.09	-0.01	0.07	-0.04	-0.01	0.03	0.81
	0.28	0.05	-0.05	0.12	-0.06	-0.06	-0.01	0.93
	0.30	0.04	-0.07	0.11	-0.03	-0.03	-0.02	0.92

Table 4. Item Loadings and Cross-Loadings (Part 2).

	AVE	CR	R^2	CA	AA	BI	TC	C	PB	TR	SA	TT
AA	1.00	1.00	0.00	1.00	1.00							
BI	0.66	0.93	0.61	0.92	-0.10	0.81						
TC	0.66	0.86	0.00	0.75	-0.01	0.39	0.82					
C	0.54	0.96	0.33	0.95	0.07	-0.48	-0.50	0.74				
PB	0.86	0.92	0.00	0.84	-0.17	0.77	0.45	-0.50	0.93			
TR	0.85	0.94	0.00	0.91	-0.05	0.35	0.49	-0.43	0.42	0.92		
SA	0.79	0.92	0.00	0.87	0.31	0.06	0.00	0.12	-0.05	-0.05	0.89	
TT	0.87	0.95	0.00	0.92	0.09	0.31	0.45	-0.43	0.36	0.52	-0.04	0.93

Table 5. Internal Consistency and Discriminant Validity of Constructs (CR = Composite Reliability, CA = Cronbachs Alpha).

We examine convergent validity by determining reliability of items, composite reliabilities of constructs and the average variances extracted (AVE) by constructs. The loadings of the items on the constructs exceed the generally accepted criterion of 0.7 (except two last items of CE, which we excluded from further consideration); therefore item reliability is met (see Table 4). Composite reliabilities of constructs and the average variances extracted (AVE) for the constructs are well above the generally accepted cut-off-values of 0.7 and 0.5, respectively, and are thus adequate (see Table 5).

Following the recommendations by Chin (1998), we examine discriminant validity by checking whether all the loadings are higher than cross-loadings (see Table 4) and the square roots of the AVE of the construct are higher than the correlation between the construct and any other construct (see Table 5). We revealed only the second item of CU to load more on CE, which we considered in our further model testing as one of the measures of CE. To approach the second condition, we removed the first item of PB which showed the highest loading on BI among all PB's indicators. Tables 4, 5 and 6 present the final results of our model testing.

5.2 Structural Model

The results of our structural model testing are presented in Table 6. The results indicate support for almost all hypotheses. Patient information privacy concerns show significant negative effect on individual's behavioral intention to accept the health cloud scenario, whereas the trust in privacy-preserving regulatory and technological mechanisms as well as cloud provider(s) in the healthcare sector can significantly reduce patient information privacy concerns. The privacy calculus components, i.e., patient information privacy concerns and perceived benefits, provide a significant competing influence on individual's behavioral intention to accept the health cloud scenario. As the path coefficients show, the perceived benefits of the health cloud scenario override the impact of patient information privacy concerns. As H5 and H6 are not supported, we can conclude that individuals do not tend to rely on their information privacy awareness, both stated and actual, in building their patient information privacy concerns.

Hypothesis	Path Estimates	Significance	Supported / Not Supported
Hypothesis 1: C -> BI	-0.120	3.128	Supported
Hypothesis 2: TT -> C	-0.198	3.633	Supported
Hypothesis 3: TR -> C	-0.152	2.546	Supported
Hypothesis 4: TC -> C	-0.335	6.329	Supported
Hypothesis 5: SA -> C	0.085	1.632	Not Supported
Hypothesis 6: AA -> C	0.050	1.116	Not Supported
Hypothesis 7: PB -> BI	0.713	21.433	Supported

Table 6. Results of Structural Model Testing (Significance at 5% Level).

6 Conclusion, Implications and Suggestions for Future Research

Drawing on different theories, i.e., the privacy calculus theory and the unified theory of acceptance and use of technology (UTAUT and UTAUT2), and previous related research, we developed a research model suggesting individuals' patient information privacy concerns are influenced by their knowledge about information privacy as well as trust in cloud providers in the healthcare sector, and privacy-preserving technological and regulatory mechanisms. Furthermore, we posited patient information privacy concerns and perceived benefits of the health cloud scenario to affect the behavioral intention to accept it. We transformed the research model into a structural equation model and empirically tested it by applying survey-based research.

The results of testing the structural equation model indicate that the trust in privacy-preserving regulatory and technological mechanisms as well as in cloud providers in the healthcare sector are the key determinants in explaining the variation in the extent to which individuals are concerned about their privacy while accepting the health cloud scenario. They all have a significant negative effect and thus can reduce them. Surprisingly, we also find that knowledge about information privacy, both stated and actual, doesn't significantly influence information privacy concerns in our scenario. A possible explanation is that the benefits which individuals expect to receive through the health cloud scenario are seen as so significant that knowledge about information privacy is ignored. In addition, our study demonstrates the evidence of the privacy calculus perspective in establishing of individuals' behavioral intention to accept the health cloud scenario. The positive aspects of health clouds outweigh concerns for patient information privacy, which is especially remarkable for the privacy-sensitive German-speaking area and immediately after the NSA scandal.

Our empirical findings about privacy concerns have implications for theory and practice. We developed a comprehensive theoretical framework explaining how individuals' patient information privacy concerns are established and form behavioral intention to accept the health clouds. For practice, the study shows how individuals' concerns for information privacy in the context of health clouds can be overcome, i.e., by building trust in privacy-preserving regulatory and technological mechanisms, and cloud providers in the healthcare sector. Even in the presence of information privacy concerns, behavioral intention to accept health clouds can be strengthened by convincing individuals of their benefits.

In our further research, we are going to formally test the direct impact of age and gender along with personal health condition on the construct of patient information privacy concerns in our research model. We will also seek to enhance the generalizability of our model by collecting empirical data from other countries.

References

Angst, C.M. and Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. MIS Quarterly, 33 (2), 339-370.

Bansal, G. and Davenport, R. (2010). Moderating Role of Perceived Health Status on Privacy Concern Factors and Intentions to Transact with High versus Low Trustworthy Health Websites. In Proceedings of the Midwest Association for Information Systems Conference.

Bansal, G., Zahedi, F. and Gefen, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online, Decision Support Systems, 49 (2), 138-150.

Belanger, F. and Crossler, R.E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35 (4), 1017-1041.

Brecht, F., Fabian, B., Kunz, S. and Müller, S. (2012): Communication Anonymizers: Personality, Internet Privacy Literacy and Their Influence on Technology Acceptance. In Proceedings of European Conference on Information Systems.

Chin, W.W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In G.A. Marcoulides (Ed.), Modern Methods for Business Research, 295-336.

Deng, M., Nalin, M., Petkovié, M., Baroni, I. and Marco, A. (2012). Towards Trustworthy Health Platform Cloud. In Proceedings of Secure Data Management.

Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research, 17 (1), 61–80.

Dinev, T., Albano, V., Xu, H., D'Atri, A. and Hart, P. (2012). Individual's Attitudes Towards Electronic Health Records – A Privacy Calculus Perspective. Annals of Information Systems, forthcoming.

Gefen, D., Straub, D.W. and Boudreua, M.C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. Communications of the Association for Information Systems, 4 (7), 1-78.

Ion, I., Sachdeva, N., Kumaraguru, P. and Capkun, S. (2011). Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage. In Proceedings of Symposium on Usable Privacy and Security.

Kaletsch, A. and Sunyaev, A. (2011). Privacy Engineering: Personal Health Records in Cloud Computing Environments. In Proceedings of International Conference on Information Systems.

Karthikeyan, N. and Sukanesh, R. (2012). Cloud Based Emergency Health Care Information Service in India. Journal of Medical Systems, 36 (6), 4031-4036.

Krasnova, H., Kolesnikova, E. and Günther, O. (2010). Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study. In Proceedings of European Conference on Information Systems.

Laric, M.V., Pitta, D.A. and Katsanis, L.P. (2009). Consumer Concerns for Healthcare Information Privacy: A Comparison of U.S. and Canadian Perspectives. Research in Healthcare Financial Management, 12 (1), 93-111.

Laudon, K. C., Laudon, J. P. and Schoder, D. (2010). Wirtschaftsinformatik - Eine Einführung. 2. aktualisierte Auflage. Pearson Studium.

Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. Communications of the Association of Information Systems, 28 (28), 453-496.

MacKenzie, S.B., Podsakoff, P.M. and Podsakoff, N.P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. MIS Quarterly, 35 (2), 293-334.

Mell, P. and Grance, T. (2012). The NIST Definition of Cloud Computing. National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed March 12, 2014.

Pavlou, P.A. (2011). State of the Information Privacy Literature: Where Are We Now And Where Should We Go? MIS Quarterly, 35 (4), 977-988.

Petter, S., Straub, D. and Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. MIS Quarterly, 33 (4), 623-656.

Poulymenopoulou, M., Malamateniou, F. and Vassilacopoulos, G. (2011). E-EPR: a Cloud-Based Architecture of an Electronic Emergency Patient Record. In Proceedings of International Conference on PErvasive Technologies Related to Assistive Environments.

Ringle, C.M., Wende, S. and Will, S. (2005). SmartPLS 2.0 (M3) Beta, Hamburg, Germany, http://www.smartpls.de. Accessed March 12, 2014.

Rohm, A.J. and Milne, G.R. (2004). Just What the Doctor Ordered – The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern. Journal of Business Research, 57 (9), 1000-1011.

Smith, H.J., Milberg, J.S. and Burke, J.S. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly, 20 (2), 167-196.

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

TRESOR (2014). TRESOR, http://www.cloud-tresor.com/. Accessed March 12, 2014.

Urbach, N. and Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. Journal of Information Technology Theory and Application, 11 (2), 5-40.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View, MIS Quarterly, 27 (3), 425–478.

Venkatesh, V., Thong, J.Y.L. and Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. MIS Quarterly, 36 (1), 157-178.

Wetzels, M., Odenkerken-Schroder, G. and van Oppen, C. (2009). Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration, MIS Quarterly 33 (1) 117-195.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems, 12 (12), 798-824.