Security and Acceptance of Cloud Computing in Healthcare

vorgelegt von

M.Sc. Wirtschaftsinformatik

Tatiana Ermakova

geboren in Moskau

von der Fakultät VII – Wirtschaft und Management

der Technischen Universität Berlin

zur Erlangung des akademischen Grades

Doktor der Wirtschaftswissenschaften

– Dr. rer. oec. –

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender: Prof. Dr. med. habil. Reinhard Busse

Gutachter: Prof. Dr. rer. pol. habil. Rüdiger Zarnekow

Gutachterin: Prof. Dr. rer. pol. habil. Hanna Krasnova

Tag der wissenschaftlichen Aussprache: 21. August 2015

Berlin 2015

Abstract

Due to the expected severe shift in the age structure of the world's population in the future, the healthcare system can be put under pressure. Since recent years, cloud computing provides significant technological advances. In healthcare, the capabilities of cloud computing can be employed to support medical treatment for high-cost diseases, especially through enabling timely sharing of medical records across various institutions involved in the treatment. However, as the extensive literature review which is conducted as part of the present work shows, there are still breaches in the existing security and privacy-preserving mechanisms. Referring to this issue, the present research examines and demonstrates that individuals' concern for privacy of medical information would inhibit acceptance of cloud computing in healthcare. The results further suggest that trust in privacy-preserving mechanisms, both regulatory and technological ones, as well as trust in cloud providers are significant factors in mitigating this concern, while perceived benefits can outweigh this concern in the decision to accept cloud computing in healthcare. In addition, this work investigates and provides empirical support that stronger confidentiality measures and assurances can actually lead to higher levels of acceptance of cloud computing in healthcare. To verify this positive influence and support this acceptance process, important security and privacy system requirements related to the considered area are deduced and addressed in a corresponding architecture design.

Aufgrund der zu erwartenden starken Verschiebung in der Altersstruktur der Weltbevölkerung in der Zukunft kann das Gesundheitssystem unter Druck geraten. In den letzten Jahren bietet Cloud Computing erhebliche technologische Fortschritte. Im Gesundheitswesen können die Möglichkeiten von Cloud Computing eingesetzt werden, um die medizinische Behandlung aufwendiger Erkrankungen zu unterstützen, vor allem dadurch, dass ein zeitnaher Austausch von medizinischen Aufzeichnungen unter verschiedenen, an der Behandlung beteiligten Institutionen ermöglicht wird. Wie die umfangreiche Literaturübersicht zeigt, die im Rahmen der vorliegenden Arbeit erstellt wurde, gibt es jedoch immer noch Lücken in den bestehenden Mechanismen zur Gewährung der Informationssicherheit und des Datenschutzes. Mit Hinblick auf dieses Problem zeigt die vorliegende Forschung empirisch auf, dass die Bedenken der Individuen bezüglich des Schutzes der medizinischen Informationen die Akzeptanz von Cloud Computing im Gesundheitswesen hemmen würden. Die Ergebnisse deuten weiterhin darauf hin, dass das Vertrauen in die Mechanismen zur Gewährung des Datenschutzes, sowohl regulatorische als auch technologische, sowie das Vertrauen in Cloud-Anbieter wesentliche Faktoren beim Mildern dieser Bedenken sind, während wahrgenommener Nutzen diese Bedenken bei der Entscheidung für Cloud Computing im Gesundheitswesen überwiegen kann. Darüber hinaus untersucht diese Arbeit und liefert empirische Belege dafür, dass stärkere Vertraulichkeitsmaßnahmen und Garantien tatsächlich zu einer höheren Akzeptanz von Cloud Computing im Gesundheitswesen führen. Um diesen positiven Einfluß zu überprüfen und einen solchen Akzeptanzprozess zu unterstützen, werden wichtige Systemanforderungen zur Informationssicherheit und zum Datenschutz abgeleitet und in einem entsprechenden Architektur-Design adressiert.

Acknowledgement

I would like to express my sincere gratitude to my academic supervisor Prof. Dr. Rüdiger Zarnekow for giving me the opportunity to work for the TRESOR research project as part of his team and to pursue a doctoral degree. It was an immense pleasure for me to be able to follow my favorite research directions under his support and guidance.

I would like to thank PD Dr. Benjamin Fabian for his encouragement, valuable advice, active guidance, and inspirations which I luckily got every time I needed them.

I also thank Prof. Dr. Hanna Krasnova for kindly examining this research and for her advice.

Finally, I would like to thank my family for their love, support, and constant encouragement over the years and dedicate this thesis to them.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ATB	Attitude toward Behavior
BI	Behavioral Intention
CFIP	Concern for Information Privacy
EHR	Electronic Health Records
EMS	Emergency Medical Service
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IUIPC	Internet User's Information Privacy Concerns
MSRA	Multilateral Security Requirements Analysis
NIST	National Institute of Standards and Technology
NS	Not Statistically Significant
PaaS	Platform as a Service
PBC	Perceived Behavioral Control
PHR	Personal Health Record
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
SaaS	Software as a Service
SE	Self-efficacy
SEM	Structural Equation Modelling
SN	Subjective Norm
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
TRESOR	TRusted Ecosystem for Standardized and Open cloud-based Resources
UTAUT	Unified Theory of Acceptance and Use of Technology

1. Introduction

1.1 Motivation

Currently, healthcare providers are confronted with increasing demands for healthcare services in the presence of limited resources (Halbe et al., 2010). Due to the projected severe change in the demographic structure of the world's population, the healthcare system might face further substantial challenges (Kochhar, 2014). According to the population projections by German Federal Statistical Office (2009) for the year 2060, the old-age (65 years and over) to working-age (20 to under 65 years) dependency ratio in Germany will almost double for potential pensioners, when compared to 2008. Moreover, as of 2008, German senior citizens showed disproportionately higher health expenditures (Statistisches Bundesamt, 2015).

Information and communication technologies are gaining higher importance with their variety of benefits (Chang et al., 2009; Chen at al., 2011; Delgado, 2011; Hoang and Chen, 2010; Izuddin et al., 2012). Since recent years, cloud computing provides further technological advances (Yang and Tate, 2012; Marston et al., 2011; Andriole, 2012; Buyya et al., 2009). It involves a business model of providing virtual machines, development tools and software on demand, usually over the Internet (Mell and Grance, 2012). A recent report by McKinsey Global Institute (Manyika et al., 2013) estimates that cloud computing applications could potentially have an annual economic impact of $1.7 trillion to $6.2 trillion in 2025.

In healthcare, cloud computing promises multiple improvements as well (Sultan, 2014a, 2014b; Haskew et al., 2015). For instance, these technological capabilities can be employed to support patients suffering from heart diseases (TRESOR, 2015) and diabetes (Berndt et al., 2012) and needing physiological treatment (Abbadi et al., 2011; Deng et al., 2011, 2012; Berndt et al., 2012). It is worth mentioning that as of 2008, the highest expenditures in the German health system resulted from treating heart diseases (37 billion euro or 14.6% of the entire costs), followed by digestive system diseases (34.8 billion euro or 13.7%) and mental and behavioral disorders (28.7 billion euro or 11.3%) (Statistisches Bundesamt, 2015). Furthermore, heart disease (40%) and cancer (25%) were the leading causes of death in 2013 in Germany (Statistisches Bundesamt, 2015). In the United States, they also led to the first and second highest mortality rates in 2008 till 2011, while diabetes and suicide were placed 7th and 10th in the rankings (Kochanek et al., 2011; Hoyert and Xu, 2012).

In general, a cloud computing environment is characterized as supporting connection (Ratnam and Dominic, 2012) and coordination (Shini et al., 2012) among medical workers, and facilitating medical data sharing (Basu et al. 2012; Guo et al. 2010; Li et al. 2011; Koufi et al. 2010; Deng et al. 2011). Nevertheless, thorough investigations of patients' perceptions surrounding health clouds are essential (Duquenoy et al., 2012). In this work, a health cloud is related to a cloud computing service used by healthcare providers mainly for storing medical information.

Previous research has examined patient support for exchange of medical records between medical workers in general and electronically. In the survey by Teixeira et al. (2011), a striking majority (84%) of 93 patients infected with HIV (human immunodeficiency virus) stated their willingness to share their health data with all clinicians involved in their care. Over 90% of the 511 patients surveyed by Perera et al. (2011) spoke in support of the computerized sharing of patients' health records among their health care professionals. In December 2011, al-

most 80 percent of one thousand US participants believed that electronic health information exchange (HIE) between healthcare providers would improve healthcare quality (Ancker et al., 2012a). In New York, a state with a six-year positive experience in HIE, there were about 70 percent of eight hundred participants who supported HIE among healthcare providers and believed it would improve healthcare quality (Ancker et al., 2012b). In the qualitative study by Simon et al. (2009), patients also generally associated HIE with improved healthcare quality and safety.

The privacy of medical records is currently addressed by various regulations such as Directive 95/46/EC of the European Parliament and of the Council (European Parliament and Council, 1995) and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (U.S. Department of Health and Human Services, 2015). Nevertheless, previous research also indicates that patients are generally anxious about the privacy of their medical records being electronically transferred. Lafky and Horan's (2011) survey participants reported expecting that "*security breaches will happen no matter what*" rather than being unworried about security or trusting that "*safeguards*" would protect their data. Half of the respondents in the study by Perera et al. (2011) reported being worried about the security of patient information more when it travelled over the Internet than when it was stored on computers. Nearly half of one thousand US responders associated HIE with worsened privacy and security (Ancker et al., 2012a). Nearly 70 percent of 800 New York responders expressed security and privacy concerns regarding HIE (Ancker et al., 2012b). In the qualitative study by Simon et al. (2009), patients were concerned about possible privacy breaches and misuse of their personal health data. In particular, the recipients of patient information were found essential for development of individuals' attitudes toward their information sharing (Whiddett et al., 2006). The qualitative interviewees by Lafky and Horan (2011) were afraid of the exposure of their health status to strangers, employers, researchers, or associates (e.g., family or friends). Perera et al. (2011) lists private insurance companies (67% of the respondents), the pharmaceutical industry (45%), the government (40%), and universities, or hospital-based researchers (22%) among the most undesirable outsiders. As investigated by Rohm and Milne (2004), medical information is at least wished to be collected and used by direct marketers.

Medical records being misused can lead to significant negative consequences for the patient (Bansal et al., 2010; Laric et al., 2009; Rohm and Milne, 2004; Cushman et al., 2010; Duquenoy et al., 2012; Appari and Johnson 2010). Interestingly, even a piece of inaccurate information is still highly likely to be enough to identify the person with the help of external information sources (Li et al., 2011d). The qualitative interviewees by Lafky and Horan (2011) viewed identity theft and potential discrimination as the result of their health status being misused. Teixeira et al. (2011) reported that almost all (96%) HIV-infected patients actually felt discriminated some of the time or more, namely as if "*society look[ed] down on people living with HIV*", whereas nearly half of those patients had that feeling most or all of the time.

Patients' trust in professionals responsible for healthcare services and information systems, the government (Duquenoy et al., 2012; Rauer, 2012) and the technology to safeguard their personal health information (Duquenoy et al., 2012) appears to be worth examining as well. Undem (2010) observes that trust in the provider of the PHR (16%), indications of Web site security (15%) and HIPAA (4%) are able to make PHR users feel that information would be kept safe and private. The 2008 BCS Data Guardianship Survey appears to show that people raise essential expectations with regards to their data protection through the government: After a series of data breaches and losses in the United Kingdom in 2008, two-thirds of British

adults felt a decreased level of trust in government departments to correctly manage their data (BCS, 2008).

The present dissertation has been written during the author's employment as a research assistant at the Department of Information and Communication Management of the Technical University of Berlin between 2012 and 2015. Within this time, the author was involved in a larger research project called TRESOR (TRusted Ecosystem for Standardized and Open cloud-based Resources) with partners from the healthcare industry. The author followed the research strategy of combining the work on the project and academic research. Referring to the insights gained from the project, the author derived research questions and showed practice-oriented implications of the obtained research results.

1.2 Research Objectives

Table 1 gives a general overview over research questions addressed and scientific works used to answer them. Figure 1 shows how these research questions are related to each other.

First of all, the current state of research in the area of cloud computing in healthcare is observed.

Research question 1: What is the state of the art of cloud computing in healthcare in research?

The conducted extensive literature review reveals that the existing security and privacy-preserving mechanisms for enabling health clouds require further development and improvement (Abbas and Khan, 2014; Abbadi et al., 2011; Deng et al., 2011; Shini et al., 2012; Loehr et al., 2010) (3 of Figure 1). Furthermore, cloud computing is associated with severe security and privacy related concerns (Deng et al., 2011, 2012; Hoang and Chen, 2010; Berndt et al., 2012; Ekonomou et al., 2011; Li et al., 2010, 2011b, 2012; Chen et al., 2012a; Shini et al., 2012; Abbadi et al., 2011; Chen and Hoang, 2011) (1 of Figure 1).

Research question 2: What determinants are responsible for explaining individuals' acceptance of health clouds?

Following the latter issue, this research attempts to better understand the balance between health information privacy concerns and perceived benefits in formation of health clouds' acceptance. Concurrently, this research elaborates on concerns about patient information privacy. In particular, it checks the role of trust in the capabilities of regulatory and technological mechanisms to preserve online privacy and trust in cloud providers in healthcare, as well as stated and actual awareness about information privacy.

The study results reveal that among other factors trust in the privacy-preserving technological mechanisms exerts a significant impact on health information privacy concerns. In the light of this finding and a similar one made by Dinev et al. (2012), this work attempts to thoroughly investigate the efficacy of stronger confidentiality measures and assurances as a means of increasing acceptance of health clouds among individuals (2 of Figure 1).

Research question 3: Can individuals' acceptance of health clouds be improved through addressing additional security and privacy system requirements?

This verification is enabled through deducing a set of related security and privacy system requirements (4 of Figure 1) and constructing a secure and privacy-friendly health cloud architecture that fulfills some of them (5 of Figure 1).

Research question 3.1: What security and privacy system requirements are to be addressed in a health cloud architecture?

In particular, the so-called multi-provider cloud architecture provides confidentiality of the stored or transmitted medical records even in the cases of compromised encryption keys and broken or insecurely implemented encryption algorithms (Ermakova and Fabian, 2013; Fabian et al., 2014). Encrypted health records are proposed to be divided into different fragments by a secret-sharing scheme (Shamir, 1979). The fragments are then to be distributed among several independent cloud services. The mechanism guarantees the reconstruction of the initial document in the presence of a given number of document shares; otherwise, the reconstruction is absolutely impossible.

Furthermore, this proposal is supposed to address the shortcomings of the previously proposed security and privacy mechanisms in this step (3 of Figure 1).

Research question 3.2: How can the security and privacy system requirements be addressed in a health cloud architecture?

Finally, the efficacy of higher increased confidentiality assurances is validated as a means of increasing acceptance of health clouds among individuals.

Research question 3.3: Does individuals' acceptance of health clouds increase when additional security and privacy system requirements are addressed?

Nr.	**Research Question**	**Section**	**Publication**
1	What is the state of the art of cloud computing in healthcare in research?	3	Ermakova et al., 2013a
2	What determinants are responsible for explaining individuals' acceptance of health clouds?	4	Ermakova et al., 2014a
3	Can individuals' acceptance of health clouds be improved through addressing additional security and privacy system requirements?		
3.1	What security and privacy system requirements are to be addressed in a health cloud architecture?	5	Ermakova et al., 2013b
3.2	How can the security and privacy system requirements be addressed in a health cloud architecture?	6	Ermakova and Fabian, 2013
3.3	Does individuals' acceptance of health clouds increase when additional security and privacy system requirements are addressed?	7	Ermakova et al., 2015b

Table 1. General Overview over Research Questions and Associated Publications Used

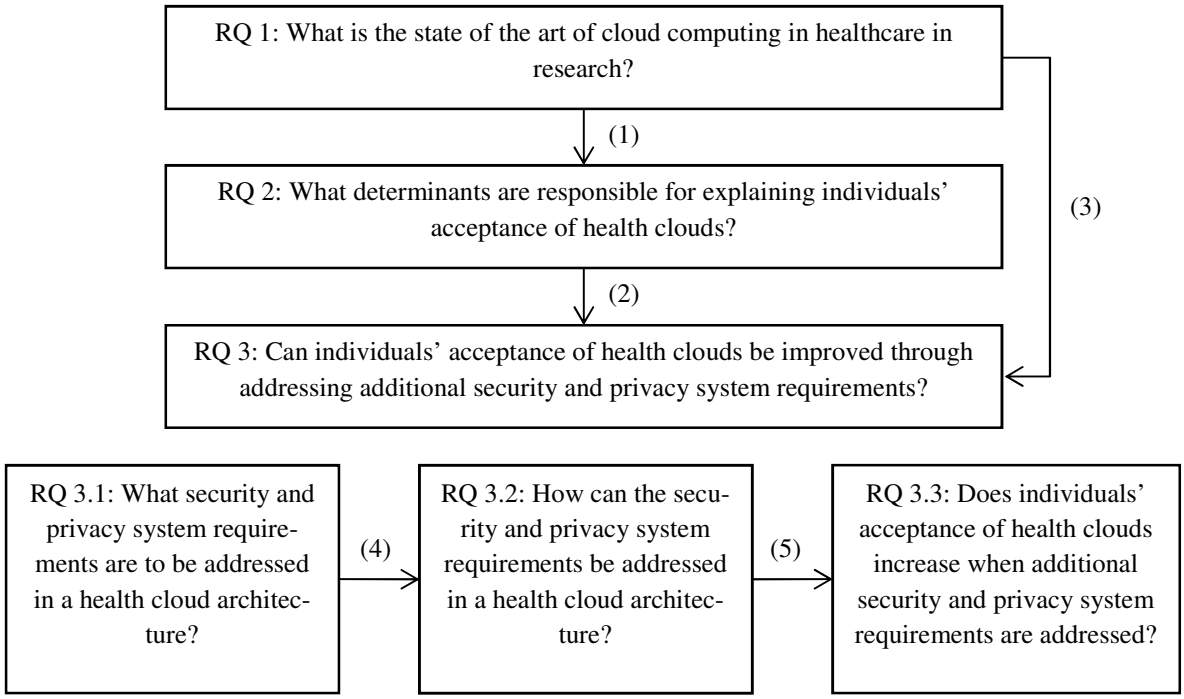

Figure 1. General Overview over Research Questions

1.3 Research Methodology

Research methodologies in the information systems (IS) discipline can be classified in terms of their research paradigm (behavioral science vs. design science) and degree of formalization (quantitative vs. qualitative) (Wilde and Hess, 2007). The behavioral-science paradigm "*seeks to develop and verify theories that explain or predict human or organizational behavior*" (Hevner et al., 2004, p. 75). The design-science paradigm is associated with creating and evaluating IT artifacts (e.g., models, methods or systems) that broaden human and organizational capabilities (Hevner et al., 2004; Wilde and Hess, 2007). Through the terms of quantitative and qualitative research, predominantly numerical representations and representations through natural language are differentiated (Wilde and Hess, 2007).

In the present work, research methodologies of different research paradigms and degrees of formalization were applied to produce research results (Table 2). These research methodologies include quantitative cross-sectional analysis (Ermakova et al., 2014a, 2014b, 2015a, 2015b), prototyping (Fabian et al., 2012; Ermakova and Fabian, 2013; Fabian et al., 2014; Slawik et al., 2014; Zickau et al., 2014), action research and reference modeling (Hanner et al., 2014), and argumentative-deductive analysis (Ermakova et al., 2013a, 2013b, 2013c). A *quantitative cross-sectional analysis* results in a cross-sectional picture of a sample, which usually allows drawing conclusions about the whole population (Wilde and Hess, 2007). For example, Ermakova et al. (2014a, 2014b) apply the partial least squares technique for testing and estimating some causal relationships. *Prototyping* implies that a preliminary version of some application system is developed and evaluated. By means of *reference modeling,* simplified and optimized pictures (ideal concepts) of systems are usually inductively (based on observations) or deductively (e.g., from theories or models) created in order to deepen existing knowledge and generate design templates. *Action research* brings researchers and practitioners together to resolve some practice issue. It may include several cycles of analysis, action

and evaluation steps where slightly structured instruments such as group discussions or planning games are used. (Wilde and Hess, 2007)

		Paradigm	
		Behavioral science	**Design science**
Degree of formalization	**Quantitative**	Ermakova et al. (2014a): quantitative cross-sectional analysis Ermakova et al. (2014b): quantitative cross-sectional analysis Ermakova et al. (2015a): quantitative cross-sectional analysis Ermakova et al. (2015b): quantitative cross-sectional analysis Ermakova (2015): quantitative cross-sectional analysis to be applied	
	Qualitative		Fabian et al. (2014): prototyping Slawik et al. (2014): prototyping Zickau et al. (2014): prototyping Hanner et al. (2014): action research, reference modeling[1] Ermakova et al. (2013a): argumentative-deductive analysis Ermakova et al. (2013b): argumentative-deductive analysis Ermakova and Fabian (2013): prototyping Ermakova et al. (2013c): argumentative-deductive analysis Slawik et al. (2012): action research, prototyping Fabian et al. (2012): prototyping

Table 2. Research Methodologies Applied (Based on Wilde and Hess (2007)) (Black: Publications Used; Grey: Other Publications)

[1] Reference modeling as applied in Hanner et al. (2014) is classified as qualitative approach due to the absence of a formal modeling language.

1.4 Overview over Publications Used

Due to its cumulative character, this dissertation is mainly comprised of several scientific papers which deal with interrelated aspects of the research topic (see Table 3). The publications were chosen based on the criteria of publication quality and coherence (see Table 28 in the appendices for the complete list of the publications of the author). To ensure high quality of the publications, we consult well-established publication rankings such as WKWI (2011) and VHB (2011) (see Table 28). To guarantee that the publications cohere with one another, we derive superordinate research objectives (see Section 1.2), present joint theoretical foundations (see Section 2) and give a combined conclusion (see Section 9).

Section		**Publication**
Nr.	**Title**	
3	Cloud Computing in Healthcare	Ermakova, T.; Huenges, J.; Erek, K.; Zarnekow, R.: Cloud Computing in Healthcare – A Literature Review on Current State of Research. 19th Americas Conference on Information Systems (AMCIS), 2013a.
4	Investigating Acceptance of Health Clouds	Ermakova, T.; Fabian, B.; Zarnekow, R.: Acceptance of Health Clouds – A Privacy Calculus Perspective. 22th European Conference on Information Systems (ECIS), 2014a.
5	Security and Privacy Requirements for Health Clouds	Ermakova, T.; Fabian, B.; Zarnekow, R.: Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios. 19th Americas Conference on Information Systems (AMCIS), 2013b.
6	Security and Privacy-Preserving Architecture for Health Clouds	Ermakova, T.; Fabian, B.: Secret Sharing for Health Data in Multi-Provider Clouds. 15th IEEE Conference on Business Informatics (IEEE CBI), 2013.
7	Evaluation of Improvement in Acceptance of Health Clouds	Ermakova, T.; Fabian, B.; Zarnekow, R.: Improving Acceptance of Health Clouds. In Submission, 2015b.
8	Discussion	Ermakova, T.: Understanding Physicians' Adoption of Health Clouds. 4th International Conference on Information Technology Convergence and Services (ITCS), 2015.

Table 3. Overview over Publications Used

1.5 Structure of This Thesis

This thesis is organized as follows: Section 2 provides theoretical foundations which are essential for the whole present research. In Section 2.1, the current and expected issues and challenges of the healthcare area are covered and some meaningful capacities of the cloud computing technology in the given context are shown. Section 2.2 gives a brief summary of some basic principles of security and secret sharing as a security-preserving mechanism. Section 2.3 deals with psychological fundamentals related to technology acceptance and its correlates privacy concerns, trust and awareness.

Section 3 represents an extensive literature review in the area of cloud computing in healthcare. Section 3.2 presents the methodology used to conduct the literature review. Section 3.3 introduces the findings in the scope of the identified research issues. Section 3.4 derives further research issues.

Section 4 examines the current state of individuals' acceptance of health clouds. Section 4.2 deduces the determinants of both acceptance of health clouds and concerns about the privacy of health information. In Section 4.3, the relations between the constructs are hypothesized in a causal model and an instrument to test the model is developed. Section 4.4 goes on the collection of empirical data, while Section 4.5 presents the results of testing the model.

In Section 5, main security and privacy system requirements are collected which are to be addressed in a health cloud. Section 5.2 introduces the background and related work. Section 5.3 describes the research design followed to elicit those requirements. Section 5.4 presents the final results.

Section 6 shows how some of the prior deduced security and privacy system requirements can be further addressed in an associated architecture. Section 6.2 provides some background on the protection of health data in a cloud computing environment. Section 6.3 presents two use case scenarios to explore further needs. Section 6.4 formulates the goals of our solution and constructs the architecture. Section 6.5 introduces and evaluates the mechanism of secret sharing.

Section 7 examines whether individuals' acceptance of health clouds can be improved when additional security and privacy system requirements are addressed. Section 7.2 provides some related background. Section 7.3 presents the research approach followed. The study results are presented in Section 7.4 and discussed in Section 7.5.

Section 8 provides a discussion on important issues. Section 8.1 notes on promoting trust. Section 8.2 elaborates on how to shed light on the relationships possibly not explored in the present research, based on well-established model selection approaches. Section 8.3 presents a research-in-progress work aimed to investigate the acceptance of health clouds from the perspective of healthcare professionals.

Section 9 shortly summarizes all results, shows the limitations of the present work and gives some recommendations for further work.

2. Theoretical Foundations

2.1 Cloud Computing in Healthcare

2.1.1 Healthcare

Today's healthcare system appears to deal with increased demand for healthcare services. In Germany in the year 2012, health expenditure increased by 2.3% (6.9 billion euros), when compared to the previous year (Statistisches Bundesamt, 2015). The number of healthcare employees increased by approximately 22.6% (or 950 thousand) since 2000, what is three times higher than in the overall economy (Statistisches Bundesamt, 2015).

An expected severe shift in the age structure will put further essential pressures on the healthcare system. In 2008, senior citizens (65 years and over) constituted 20 percent of the German population, while the working-age population (20 to under 65 years) formed 61 percent (Statistisches Bundesamt, 2015). According to population projections for the year 2060, the old-age to working-age dependency ratio will almost double for potential pensioners (Federal Statistical Office, 2009). Moreover, as of 2008, Statistisches Bundesamt (2015) observes disproportionately higher health expenditures for older people: People aged 65 to 84 years and older than 84 years showed the values of costs of illness per capita which were 2.1 and 4.8 times as high as the average, respectively.

2.1.2 Cloud Computing

Cloud computing emerges as a fundamental paradigm shift in the way how to invent, develop, deploy, scale, update, maintain and pay for information technology services (Marston et al., 2011). It is seen among doubtless information technology trends to define the future (Andriole, 2012; Buyya et al., 2009). Buyya et al. (2009) even anticipate viewing cloud computing as the fifth utility one day, after water, electricity, gas, and telephone.

Many scholars and practitioners have attempted to exactly define the term of cloud computing. The US National Institute of Standards and Technology (NIST) describes cloud computing as a "*model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*" (Mell and Grace, 2011, p. 2). Mell and Grace essentially characterize cloud computing through on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. According to Armbrust et al. from the University of California (Berkley), cloud computing refers to "*both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services*" (Armbrust et al., 2009, p. 1). Armbrust et al. (2009) claim that cloud computing creates the illusion that infinite computing resources are available on demand, eliminates the necessity of up-front commitments, and gives the possibility to pay for computing resources used on a short-term basis as needed. Buyya et al. (2009, p. 601) associate a cloud with "*a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers*". Hardware virtualization implies that multiple operating

systems and software stacks run on one single physical platform (Buyya et al., 2011, p. 10). Buyya et al. (2011, p. 4) suggest that the most notable common characteristics for a cloud include (1) pay-per-use, (2) elastic capacity along with the illusion of infinite resources, (3) self-service interface, and (4) abstracted or virtualised resources. Buyya et al. (2011, pp. 16-17) emphasizes that cloud computing withdraws up-front commitments by users. With short-term pricing, users are allowed to request and use resources only to the necessary amount, and release them as soon as they don't need them. Resources are further expected to be additionally provisioned and released (scaled up and down) with an application's load increases and decreases. Following Marston et al. (2011, p. 177), cloud computing represents "*an information technology service model where computing services (both hardware and software) are delivered on-demand to customers over a network in a self-service fashion, independent of device and location. The resources required to provide the requisite quality-of-service levels are shared, dynamically scalable, rapidly provisioned, virtualized and released with minimal service provider interaction. Users pay for the service as an operating expense without incurring any significant initial capital expenditure, with the cloud services employing a metering system that divides the computing resource in appropriate blocks*".

There are four main deployment models of cloud computing. They involve private cloud, community cloud, public cloud, and hybrid cloud. A public cloud is openly used by the general public, while a private cloud is exclusively utilized by a single organization and a community cloud is shared by several organizations within a community. A combination of two or more types of clouds results in a hybrid cloud. The cloud infrastructures may be owned, managed, and operated by different independent third-parties and/or related organizations. (Mell and Grace, 2011; Marston et al., 2011) Compared to the hybrid cloud approach, the multi-cloud notion used in this work refers to the amount of clouds linked together, rather than multiple deployment modes. Here, for example, data can be stored in parallel or distributed over several independent clouds for higher availability and redundancy (Petcu, 2013).

The service models of cloud computing include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Through the service models, a consumer is provided with applications (SaaS) (e.g., Salesforce.com), programming (PaaS) (e.g., Google AppEngine) and computing resources (e.g., processing, storage, networks) (IaaS) (e.g., Amazon Web Services). (Mell and Grace, 2011; Buyya et al., 2011, pp. 13-15; Marston et al., 2011)

2.1.3 Cloud Computing in Healthcare

Multiple opportunities and enhancements are supposed to be achieved due to the cloud-computing technology in the healthcare and medical service delivery.

Nowadays, access to medical records during healthcare service delivery is rather limited (Kanagaraj and Sumathi, 2011; Karthikeyan and Sukanesh, 2012; Koufi et al., 2010; Poulymenopoulou et al., 2011; Rolim et al., 2010), although their availability is regarded as crucial, in particular under emergency conditions (Karthikeyan and Sukanesh, 2012; Poulymenopoulou et al., 2011; Rolim et al., 2010). Cloud computing offers capabilities to resolve these issues. It is associated with enhanced availability, recovery and transfer of medical records (Nematzadeh and Camp, 2010), easy, immediate and ubiquitous access to medical records (Chen and Hoang, 2011; Chen et al., 2012; Hoang and Chen, 2010; Koufi et al., 2010; Loehr et al., 2010; Poulymenopoulou et al., 2011) and IT resources (Chowdhary et al., 2011; Fernández-Cardeñosa et al., 2012; Karthikeyan and Sukanesh, 2012).

Furthermore, cloud computing appears to provide an appropriate environment for connection (Ratnam and Dominic, 2012) and coordination purposes (Shini et al., 2012) among medical workers, patients, and other involved parties. In particular, cloud computing is expected to facilitate exchange of medical records (Basu et al., 2012; Guo et al., 2010; Li et al., 2011; Deng et al., 2011; Koufi et al., 2010). These capabilities can be exemplarily demonstrated through the scenarios of cloud-based home healthcare systems aimed to support depressed patients (Abbadi et al., 2011; Deng et al., 2011, 2012), elderlies (FEARLESS), patients suffering from diabetes (M-Diab) and skin (M-Skin) diseases and needing a physiological control (M-Stress, M-Fitness) (Berndt et al., 2012), and to monitor artificial-heart patients (TRESOR, 2015).

Hospitals are currently confronted with large amounts of medical data which continually increase due to technological advances and which are to be archived in a long term, even after accomplishing the patient's treatment (Huang et al., 2011; Nordin et al., 2011, 2012; Nordin and Hassan, 2011; Winter et al., 2006; Fabian et al., 2015). With respect to this, healthcare applications and medical data are supposed to be hosted and provisioned from the cloud computing environment (Basu et al., 2012; Berndt et al., 2012; Chang et al., 2009; Deng et al., 2012; Ekonomou et al., 2011; Guo et al., 2010; Wang und Tan, 2010), where adequate storage capacities for medical resources are available (Li et al., 2011; Shini et al., 2012). Cloud computing could even enable central storage for medical data (Li et al., 2011b, 2012; Shini et al., 2012).

Finally, cloud computing is believed to reduce IT costs for healthcare providers (Chen et al., 2012; Deng et al., 2011; Hoang and Chen, 2010; Loehr et al., 2010; Mohammed et al., 2010; Shini et al., 2012). Constructing an independent hospital information system implies high costs and waste of resources what should make a cloud computing solution a more preferable option (He et al., 2010; Kanagaraj and Sumathi, 2011; Li et al., 2012).

2.2 Security

The 2014 Data Breach Investigations Report (Verizon, 2014) revealed that healthcare organizations mostly suffered from hardware theft or loss (46% of all security incidents). In another 15% of the cases, employees, ex-employees or partners misused their access rights. Further 12% of incidents covered miscellaneous errors where security was compromised.

In a general sense, security is associated with the protection of assets (e.g., the contents of a file or a server) (Common Criteria, 2012; Andress, 2014, p. 3). Information security refers to protecting information as well as the systems and hardware involved in the usage, storage and transmission of that information. Information security can be enabled through applying some policy, training and awareness programs, and technology (Whitman and Mattord, 2013, p. 4). Security services involve data confidentiality, data integrity, data availability, access control, authentication, and nonrepudiation (Stallings, 2010, p. 9-10). Data confidentiality protects messages from being disclosed to an unauthorized party. Data integrity assures that messages are received as sent. Authentication assures that each party involved in a communication is who it claims to be. Nonrepudiation prevents any party involved in a communication from denying having participated in that communication. Furthermore, there are different security mechanisms to address the security services, e.g., encryption, digital signature, access control (Stallings, 2010, p. 12-13). Encryption transforms and recovers data depending on a mathematical algorithm and one or more encryption keys. Through encryption, data confidentiality,

data integrity, and authentication can be guaranteed. Digital signatures ensure authentication, data integrity, and nonrepudiation.

This thesis applies a fundamental cryptographic mechanism which is called secret-sharing scheme. A secret-sharing scheme is generally defined as a (t, n)-threshold scheme (with t and n being two positive integers) which assumes that the secret is discretely distributed in form of information pieces (also called shares) to a set of n participants, so that any subset of t or more participants can reconstruct the secret from their pieces, but any subset of t-1 or fewer participants cannot do so. (Stinson, 1992; Beimel, 1996) The secret-sharing issue was independently studied by two researchers in 1979. George Blakley (1979) relied on finite geometries, while Adi Shamir (1979) based on polynomial interpolation (Stinson, 1992). As the result of the investigations, Blakley represented shares as hyperplanes and the secret as the point of their intersection, while Shamir defined shares as points of a polynomial and the secret as the y value of the point where the polynomial crosses the y axis (see Figure 2). (Ermakova, 2011)

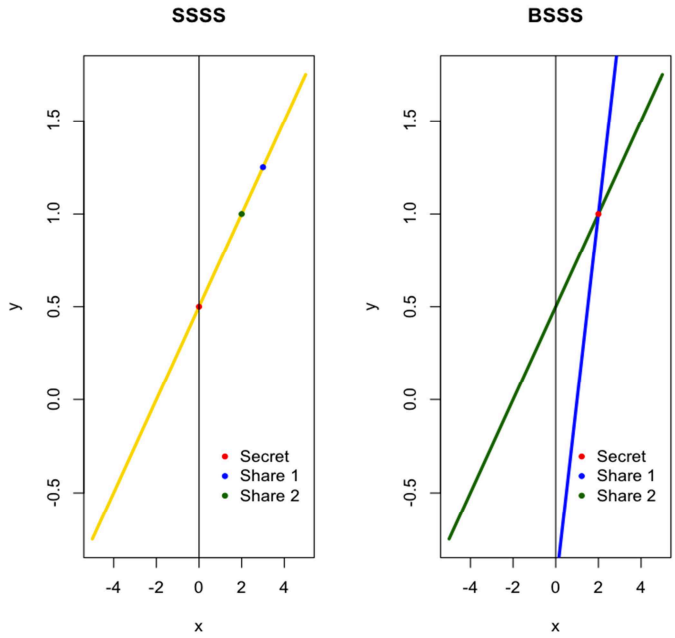

Figure 2. Shamir's (1992) Secret-Sharing Scheme (SSSS) vs. Blakley's (1979) Secret-Sharing Scheme (Ermakova, 2011)

Figure 3 shows how a secret-sharing scheme works in the practice, based on Shamir's secret sharing scheme. The mechanism creates a polynomial, while taking the secret as the first coefficient (1a) and picking the remaining coefficients at random (1b). Next, n points randomly found on the curve of the polynomial are distributed among the participants (1c). When at least t participants combine their points (2a), the polynomial can be easily reconstructed (2b) and the secret can be found as the first coefficient of the polynomial (2c).

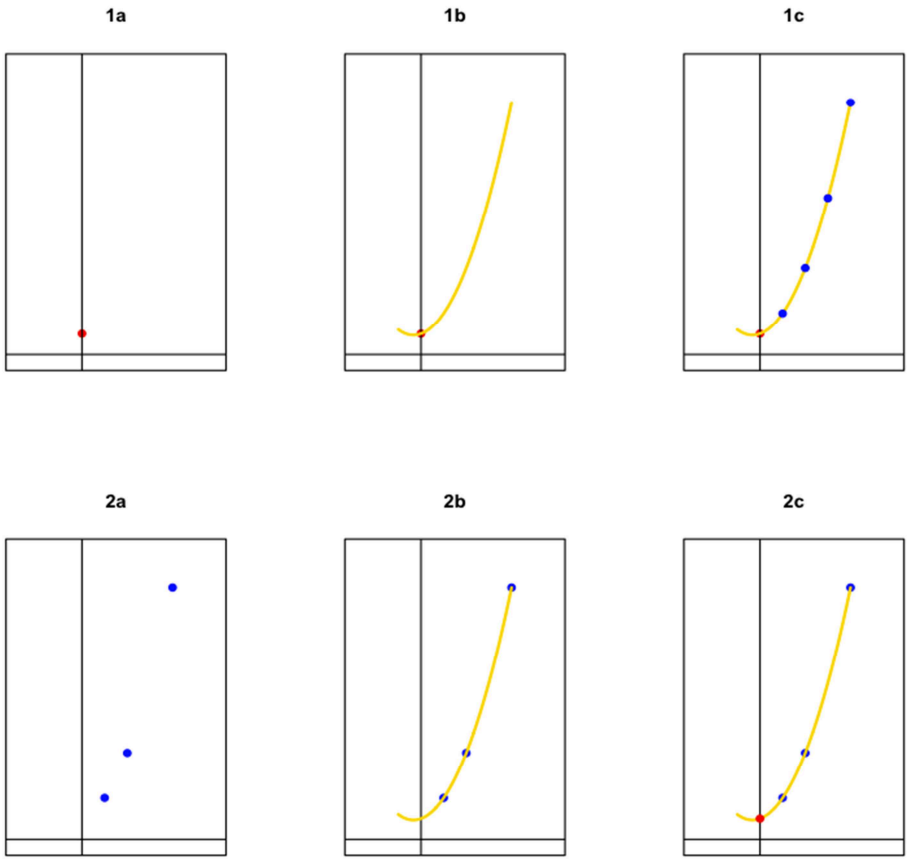

Figure 3. Shamir's (1992) Secret-Sharing Scheme (Ermakova, 2011)

In 1989, Michael O. Rabin introduced an information dispersal algorithm. In comparison to Shamir (1979) who defined the free coefficient of a polynomial by the secret, Rabin proposed to take all coefficients equal to different parts of the secret. It is worth noting that Shamir's secret-sharing scheme ensures that the secret remains absolutely undetermined in the presence of t-1 or fewer shares (perfect secrecy), while Rabin's information dispersal algorithm generates shares which are t times smaller than the original document (space efficiency).

2.3 Technology Acceptance and its Correlates - Privacy Concerns, Trust and Awareness

2.3.1 Technology Acceptance

For specifying the factors that lead an individual to accept or reject a technology, MIS scholars draw on theories such as theory of reasoned action (TRA) (Ajzen and Fishbein, 1980), theory of planned behavior (TPB) (Ajzen, 1991), technology acceptance model (TAM) (Davis, 1989), and unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003).

TRA contends that an individual' actual behavior results from his/her intention to perform some behavior (BI) which can be predicted by attitude toward that behavior (ATB) and subjective norm (SN). In addition to them, TBA considers the concept of perceived behavioral

control (PBC) which refers to the extent an individual perceives the behavior as easy or difficult to perform. TBA suggests that PBC plays a role in formation of BI and ATB.

TAM can be also considered as rooted in TRA. It similarly postulates that an individual's behavioral intention to use a technology influences actual usage behavior. The two key factors the TAM model is known for include perceived ease of use (PEOU) and perceived usefulness (PU). PEOU refers to the degree to which the user expects limited efforts regarding the usage of the technology. PU reflects the degree to which a person anticipates enhancements of his/her job performance through the usage of the technology. Along with ATB, both PU and PEOU are seen as predictors of BI. TAM further claims that PEOU is essential for PU, while PU influences ATB. TAM was further deepened in the sense of explaining PU (Venkatesh and Davis, 2000) (known as TAM2) and PEOU (Venkatesh and Bala, 2008) (known as TAM3).

UTAUT (Venkatesh et al., 2003) represents a synthesis of eight models, namely theory of reasoned action (TRA), theory of planned behavior (TPB), technology acceptance model (TAM), combined technology acceptance model and theory of planned behavior, motivational model, PC utilization model, innovation diffusion theory, and social cognitive theory (see Section 2.3.2). UTAUT was found to outperform each of these single models with R^2 of 68 percent. More specifically, UTAUT states that performance expectancy, effort expectancy and social influence affect behavioral intention to use, which, along with facilitating conditions, influences actual usage. UTAUT2 (Venkatesh et al., 2012) extends the UTAUT framework by integrating hedonic motivation, price value, and habit as determinants of behavioral intention, the last one also as a determinant of use behavior. UTAUT2 additionally proposes a path from facilitating conditions to actual behavior.

To date, multiple empirical studies confirm that behavioral intention is determined through individuals' *privacy concerns* (Angst and Agarwal, 2009; Li, 2013; Dinev and Hart, 2006b; Brecht et al., 2012; Ermakova et al., 2014a; Smith et al., 1996; Dinev et al., 2006a, 2008; Bansal et al., 2007, 2010; Korzaan and Boswell, 2008), *trust* (Dinev and Hart, 2006a; Bansal et al., 2008a, 2008b; Bansal et al., 2007, 2010; Malhotra et al., 2004; Gefen, 2000, 2002, 2003; Gefen and Straub, 2004; Dinev et al., 2006a) and *awareness* (Dinev and Hu, 2005; Dinev and Hu, 2007; Dinev et al., 2006b, 2009). Interestingly, privacy concerns were found both to be impacted by trust (Pavlou et al., 2007; Dinev et al., 2012; Ermakova et al., 2014a) and to have an impact on trust (Bansal and Zahedi, 2010; Bansal et al., 2010 (NS); Bansal, 2011a; Malhotra et al., 2004; Ermakova et al., 2014b). The notion of awareness was tested and shown to be relevant with regards to privacy concerns (Dinev and Hart, 2004, 2006b; Xu et al., 2008; Brecht et al., 2012; Ermakova et al., 2014a (NS)), and trust-related factors (Ermakova et al., 2014b). These concepts of privacy concerns, trust and awareness will be presented and discussed in detail in subsequent sections (see Sections 2.3.2, 2.3.3, and 2.3.4).

2.3.2 Privacy and Privacy Concerns

Since over 100 years, the term of general privacy has been extensively examined across different disciplines including law (Warren and Brandeis, 1890), political (Westin, 1967) and economical (Davies, 1997) sciences, psychology (Altman, 1975; Laufer and Wolfe, 1977), and management information systems (MIS) (Smith, 1996; Milne and Rohm, 2000; Malhotra et al., 2004; Son and Kim, 2008; Dinev and Hart, 2004, 2006a; Dinev et al., 2006a, 2013; Xu, 2007; Xu et al., 2011, 2012; Smith et al., 2011; Bélanger and Crossler, 2011; Pavlou, 2011). Nevertheless, there is still no final consensus among scholars about what the concept means (Pavlou, 2011; Smith et al., 2011; Dinev et al., 2013).

The multiple approaches to define general privacy are broadly classified by Smith et al. (2011) as either value-based approaches conceptualizing general privacy as a right (Warren and Brandeis, 1890) or as a commodity (Davies, 1997) or cognate-based approaches viewing general privacy as a state (Westin, 1967; Laufer and Wolfe, 1977) or as a control (Westin, 1967; Altman, 1975; Smith et al., 1996). Although equating privacy with control was followed in many MIS studies (Smith et al., 1996; Malhotra et al., 2004; Hong and Thong 2013), many researchers argue that control rather plays a key role in formation of general privacy and is thus not identical to it (Laufer and Wolfe, 1977; Dinev and Hart, 2004 (NS); Dinev et al., 2012, 2013; Xu, 2007; Xu et al., 2008, 2011, 2012).

Although present literature does not clearly distinct between physical and information privacy (Smith et al., 2011; Dinev et al., 2013), this work focuses on information privacy. With the advent of the advanced information and telecommunication technologies, data became easily collected, analyzed and utilized by multiple parties, making information privacy a matter of concern among Internet users (Davies, 1997; Malhotra et al., 2004; Smith et al., 2011; Bélanger and Crossler, 2011; Pavlou, 2011). Information privacy concerns usually refer to the degree to which individuals are concerned about online companies' practices with respect to the collection and use of their personal information (Malhotra et al., 2004; Smith et al., 1996; Son and Kim, 2008; Xu et al., 2012). In a recent study by TRUSTe (2015), nine out of ten Americans and Britons responded that they were concerned about their online privacy. When compared to the previous year, 74% of Americans and 62% of Britons expressed even higher information privacy concerns, attributing their increase in information privacy concern over the last year to the companies sharing their personal information with third parties (58% and 60%), tracking their online behavior (47% and 54%) and location on their smartphone (24% and 19%), the media reports of government surveillance programs such as NSA's PRISM (38% and 20%), as well as the privacy policies of social media networks like Facebook (29% and 27%) and search engines such as Google (both 21%).

A series of studies have paid attention to privacy concerns related to the collection and use of personal information and shown them to substantially negatively influence individuals' personal *beliefs* (e.g., trust beliefs (Bansal and Zahedi, 2010; Bansal et al., 2010 (NS); Bansal, 2011a; Malhotra et al., 2004; Ermakova et al., 2014b), risk beliefs (Cocosila et al., 2009; Malhotra et al., 2004), perceived uncertainty (Pavlou et al., 2007)), *attitudes* (Angst and Agarwal, 2009; Dinev et al., 2012), *behavioral intention* (e.g., behavioral intention to use some service (Angst and Agarwal, 2009; Li, 2013; Dinev and Hart, 2006b; Brecht et al., 2012; Ermakova et al., 2014a), behavioral intention to share information for transactions (Smith et al., 1996; Dinev et al., 2006a, 2008; Bansal et al., 2007, 2010; Korzaan and Boswell, 2008)), and *actual behavior* (Son and Kim, 2008). These results can be also observed in practice. As stated by TRUSTe (2015), almost ninety percent of both US and British Internet users admit avoiding companies that do not protect their privacy.

As identified by Li (2011), the most often analyzed antecedents of privacy concerns include *individual factors* (demographic factors, personality traits (Bansal and Zahedi, 2010; Bansal, 2010, 2011a, 2011b; Korzaan and Boswell, 2008; Brecht et al., 2012), personal knowledge and experience (Yao et al., 2007; Dinev and Hart, 2004, 2006b; Xu et al., 2008; Brecht et al., 2012; Ermakova et al., 2014a (NS))), *psychological and social-psychological factors* (e.g., perceived vulnerability or Internet risks (Dinev and Hart, 2004, 2006a; Dinev et al., 2006, 2013; Xu et al., 2008, 2011), perceived ability to control (Dinev and Hart, 2004 (NS); Dinev et al., 2012, 2013; Xu, 2007; Xu et al., 2008, 2011, 2012), perceived ability to cope with privacy threats (Yao et al., 2007), trust (Pavlou et al., 2007; Dinev et al., 2012; Ermakova et al., 2014a), perception of intrusion (Xu et al., 2008; Bansal et al., 2010), disposition to value pri-

vacy (Xu et al., 2011; Li, 2013), need for privacy (Yao et al., 2007)), *social-relational factors* (e.g., social norms (Xu et al., 2008)), *organizational and task environmental factors* (e.g., social presence and website informativeness (Pavlou et al., 2007), website familiarity and reputation (Li, 2013)), *macro-environmental factors* (cultural values (Bansal et al., 2007) and government regulatory structures), *information contingences* (types of information (Rohm and Milne, 2004; Laric et al., 2009), information sensitivity (Bansal et al., 2007, 2010)).

MIS researchers developed approaches how to measure the information privacy construct in order to test relationships in quantitative models. The most used scales to measure information privacy concerns include: *Concern for Information Privacy (CFIP)* (Smith et al., 1996) or *Internet User's Information Privacy Concerns (IUIPC)* (Malhotra et al., 2004). CFIP includes four dimensions of information privacy: collection of data, unauthorized secondary use of data, improper access to data, and errors in data. The three dimensions of IUIPC are: control over data, awareness of organizational privacy practices, and collection of data. Through a recent series of empirical studies, Hong and Thong (2013) conclude that Internet privacy concerns (IPC) conceptualized as third-order factors generally perform better than their alternatives of lower orders. The third-order factor of IPC, which had the best fit with the data contained two second-order factors of interaction management and information management, and six first-order factors of collection, secondary usage, and control (related to interaction management), errors, and improper access (related to information management), and awareness. Hong and Thong (2013) further call for phrasing the items with focus on ones' concerns for others' behavior rather than their expectations of others' behavior.

Li (2012) observes that the existing theories generally study the origin, influential factors and behavioral consequences of individuals' privacy concerns, both separately and in conjunction with other factors. Theories based on the origin of individuals' privacy concerns include *agency theory* (Pavlou et al., 2007) and *social contract theory* (Bansal et al., 2010; Culnan and Amstrong, 1999; Malhotra et al., 2004). Agency theory suggests that the problem between principals (e.g., customers) and agents (e.g., websites) arises due to the principal having incomplete and asymmetric information about the agent's behavior and the agent having the opportunity to follow his/her own interests regardless of the principal's interests. Social contract theory postulates that people's revealing of personal information to a company implies a social contract obliging the company to fairly handle that information.

Li (2012) distinguishes between individual and institutional factors influencing privacy concerns. Theories studying individual influential factors of privacy concerns involve *protection motivation theory* (Chai et al., 2009; Xu et al., 2011), *information boundary theory* (Xu et al., 2008; Rohm and Milne, 2004), *social cognitive theory* (Chai et al., 2009), and *personality theories* (Bansal et al., 2010; Korzaan and Boswell, 2008; Son and Kim, 2008). Protection motivation theory posits that an individual's intention to protect him-/herself from a given threat depends on the individual's perception of the threat's severity and probability, his/her ability to prevent it and that preventive behavior's efficacy. Information boundary theory suggests that the information to share is determined by the boundaries of an individual's information space. Social cognitive theory posits that personal factors related to cognitive, affective, biological, behavioral and environmental events determine a person's behavior. Personality theories stress the role of personality traits (e.g., psychological) in privacy perceptions and related actions.

Among theories concentrating on institutional influential factors of privacy concerns, Li (2012) identifies *procedural fairness theory* (Culnan and Amstrong, 1999; Xu et al., 2011), *social presence theory* (Pavlou et al., 2007), and *social response theory* (Culnan and Am-

strong, 1999; Zimmer et al., 2010). Procedural fairness theory suggests that people are willing to reveal their personal information to companies and let them use that information when fair information-handling procedures are in place. Social response theory suggests that people are willing to reveal personal information to a person or organization in return for a similar disclosure from them. From the perspective of social presence theory, privacy concerns can be mitigated in the presence of an appropriate social presence referring to the extent to which a consumer perceives the online interaction with a seller close to a physical one.

With respect to behavioral consequences, privacy concerns were investigated within *theory of reasoned action (TRA)* (Ajzen and Fishbein, 1980) and *theory of planned behavior (TPB)* (Ajzen, 1991) (Angst and Agarwal, 2009; Dinev and Hart, 2004, 2006a, 2006b; Malhotra et al., 2004). Based on the expectancy-value theory, TRA suggests that attitude toward a behavior (ATB) and subjective norm (SN) determine behavioral intention to perform that behavior, which in turn determines actual behavior. Developed from TRA, TBA suggests that behavioral intention to perform a behavior is additionally determined by perceived behavioral control (PBC) defined as ability to perform the behavior.

The impact of joint privacy concerns and other factors on individuals' behavior was addressed within *privacy calculus theory* (Dinev and Hart, 2006a; Hann et al., 2007; Laufer and Wolfe, 1977), *utility maximization theory* (Bansal et al., 2010; Dinev and Hart, 2006a; Hann et al., 2007), *expectancy theory of motivation* (Dinev and Hart, 2006a; Hann et al., 2007), and *expectancy-value theory* (Angst and Agarwal, 2009; Dinev and Hart, 2006a, 2006b; Malhotra et al., 2004). Privacy calculus theory suggests that an individual forms his/her intention to reveal personal information by considering the trade-off between expected negative and positive outcomes within a specific context. Utility maximization theory posits that an individual attempts to maximize his/her total utility, whereas the utility function in terms of privacy can be given by privacy calculus. Expectancy theory of motivation suggests that the higher desirability of a given outcome leads to increased motivation to behave suitably. The expectancy-value theory postulates an individual's attitude towards an object or action results from the individual's beliefs about them. The expectancy-value theory formed the basis of the above considered TRA and TPB.

2.3.3 Trust

Trust has been investigated from different perspectives, including economics and management information systems (Pavlou et al., 2007). In one of the earliest empirical studies, Mayer et al. (1995) define trust as a trustor's willingness to be vulnerable to the actions of the trustee based on his/her expectations that the trustee will accomplish some important action, regardless of the trustor's monitoring and controlling ability. Overall trust is considered separate from trustworthiness which consists of three primary dimensions: ability, benevolence, and integrity. Ability refers to the extent to which the trustee is believed to have the skills and competencies to fulfill the promises. Benevolence reflects to which extent the trusted party is assumed to have good intentions besides seeking profit. Integrity refers to the extent to which the trustee is assessed to adhere to principles acceptable for the trustor. MIS researchers mostly rely on these three dimensions when conceptualizing trust itself, although there are several other ones (Pavlou et al., 2007). Indeed, Gefen and Silver (1999) consider trust as willingness to depend based on beliefs in the trustee's ability, benevolence, and integrity, while McKnight et al. (1998, 2002) speak about trust in terms of trusting beliefs dealing with benevolence, competence, honesty, and predictability that lead to a trusting intention. Pavlou et al. (2007, p. 115) conceptualize trust as "*a buyer's intentions to accept vulnerability based on her beliefs*

that the transaction will meet her confident transaction expectations due the seller's competence, integrity, and benevolence". As stated by TRUSTe (2015), 55% of US and British internet users trusted online businesses in December 2013, what is 2% less than in January 2013.

A series of studies have shown trust to substantially negatively influence individuals' personal *beliefs* (e.g., perceived information asymmetry, fears of seller opportunism, information security concerns (Pavlou et al., 2007), information privacy concerns (Pavlou et al., 2007; Dinev et al., 2012; Ermakova et al., 2014a), perceived Internet risks (Gefen, 2002; Dinev and Hart, 2006a; Malhotra et al., 2004)), *attitude* (Jarvenpaa et al., 1999, 2000), *behavioral intention* (e.g., behavioral intention to share information for transactions (Dinev and Hart, 2006a; Bansal et al., 2008a, 2008b; Bansal et al., 2007, 2010; Malhotra et al., 2004), behavioral intention to transact (Gefen, 2000; Gefen et al., 2003; Gefen and Straub, 2004; Dinev et al., 2006a), and behavioral intention to recommend others (Gefen, 2002)). Gefen et al. (2003) show that among perceived usefulness (PU) and perceived ease of use (PEOU), experienced consumers rely on their trust in the e-vendor in building intentions to transact with the vendor again. Along with familiarity with the Internet vendor and its procedures, Gefen (2000) shows that trust in the vendor influence inquiry and especially purchase intentions on book-selling sites. A similar conclusion is done by Gefen and Straub (2004) with the exception that they considered e-trust as a multi-dimensional construct (integrity, predictability, ability, benevolence) and showed that only its integrity and predictability dimensions significantly influence purchase intentions in e-commerce. Jarvenpaa et al. (1999, 2000) show a positive effect of trust in the Internet store on the attitude toward it. Gefen (2002) concludes that trust in an online vendor is an antecedent of perceived risk with the vendor and customer loyalty.

A large number of factors were studied in terms of their formation of individual's trust. These are mainly *individual factors* (personal knowledge and experience (Ermakova et al., 2014b)), *organizational and task environmental factors* (e.g., institution-based structural assurances and situational normality (Gefen et al., 2003; McKnight et al., 2002), website familiarity (Gefen, 2000; Gefen et al., 2003 (NS)), website design (Bansal et al., 2008a, 2008b; Bansal, 2011a), website reputation (Jarvenpaa et al., 1999, 2000; Bansal et al., 2008a, 2008b; Bansal, 2011a), website information quality, availability of the company's information, adequacy (Bansal et al., 2008a, 2008b) and understandability of the website privacy policy statement (Bansal et al., 2008a, 2008b; Ermakova et al., 2014b), service quality in terms of reliability, assurance and responsiveness (Gefen, 2002), perceived size (Jarvenpaa et al., 1999, 2000)), *psychological and social-psychological factors* (e.g., calculative-based views (Gefen et al., 2003), disposition to trust (Gefen, 2000; Gefen and Straub, 2004; Dinev et al., 2006a (NS); McKnight et al., 2002), Internet Users Information Transmission Security Concerns (IUITSC) (Bansal, 2011a, 2011b), privacy concerns (Bansal and Zahedi, 2010; Bansal et al., 2010 (NS); Bansal, 2011a; Malhotra et al., 2004; Ermakova et al., 2014b), perceived Internet risks (Dinev and Hart, 2006a; Dinev et al., 2006a; Bansal et al., 2010), prior positive experience with the website (Bansal et al., 2010)), and *macro-environmental factors* (e.g., perceived effectiveness of technological mechanisms, perceived effectiveness of regulatory mechanisms (Dinev et al., 2012)). The study by Gefen et al. (2003) reveals that trust in the e-vendor is significantly influenced by the belief that the vendor cannot benefit from cheating (calculative-based views) as well as the perceptions that the Web site employs safety mechanisms (institution-based structural assurances) and has a typical and easy-to-use interface (institution-based situational normality). Familiarity with the e-vendor was found to be significantly correlated with trust in the e-vendor. However, with the above mentioned factors to be included in the research model, the effect of familiarity with the e-vendor on trust in the e-vendor was shown to be fully mediated through the perceived ease of use of the Web site, although this result can be at-

tributed to addressing familiarity with the e-vendor being gained rather through visiting the site. On the contrary, in the study by Gefen (2000), trust in an Internet vendor was found to be significantly affected by familiarity with the vendor and its procedures, this in conjunction with disposition to trust. Gefen (2002) shows that trust in an Internet vendor can be primarily build based on customer joint assessments about the vendor providing the ordered service on time (reliability), and showing knowledge and courteousness (assurance), e.g., through appropriate help screens and/or error messages, and willingness to help customers (responsiveness). The perceptions about appealing physical facilities and neatly dressed human service providers (tangibles) and individualized attention (empathy) were found to be not essential in the formation of trust in the vendor. Jarvenpaa et al. (1999, 2000) show that consumer initial trust in an Internet store positively relates to its perceived size and, more strongly, perceived reputation. Further essential factors are a website design and reputation (Bansal et al., 2008a, 2008b; Bansal, 2011a), IUITSC (Bansal, 2011a, 2011b). Understandability and adequacy of the website privacy policy statement, website information quality, availability of the company's information were found to influence trust, depending on the context (Bansal et al., 2008a) and level of privacy concerns (Bansal et al., 2008a, 2008b), while third party assurance did not significantly impacted trust (Bansal et al., 2008a, 2008b). Dinev and Hart (2006a) demonstrate that perceived Internet risks exert an impact on Internet trust. Dinev et al. (2006a) similarly show that perceived Internet risks determine institutional trust, while propensity to trust does not.

2.3.4 Awareness

In the MIS privacy-related research, there are many notions of individual being knowledgeable regarding information and communication technologies. They include Internet literacy (Dinev and Hart, 2006b; Dinev, 2008), Internet technical literacy (Dinev and Hart, 2004), Internet privacy literacy (Brecht et al., 2012; Ermakova et al., 2014b), as well as technology awareness (Dinev and Hu, 2005, 2007; Dinev et al., 2006b; Dinev et al., 2009), social awareness (Dinev and Hart, 2004; Dinev and Hart, 2006b; Dinev, 2008), privacy awareness (Xu et al., 2008; Brecht et al., 2012; Ermakova et al., 2014a), and self-efficacy (Dinev and Hu, 2005, 2007; Dinev et al., 2009). Internet literacy refers to individual ability to use computers connected to the Internet and applications of the Internet to perform practical tasks. Internet technical literacy (or Internet privacy literacy) measures a higher level of Internet users' usage and extends Internet literacy by one's skills to handle Internet threats. Awareness measures the extent to which one follows, shows interest in, and knows about policies and initiatives issued by the community and government, among others with regards to technology and the Internet (social awareness), or technological problems and techniques to address them (technology awareness), or privacy practices and policies, how disclosed information is used and impacts one's privacy-preserving ability (privacy awareness). Self-efficacy (SE) reflects individual judgment of his/her skills and capabilities to accomplish a certain behavior.

Internet literacy was found to negatively influence privacy concerns (Dinev and Hart, 2006b) and perceived need for government surveillance (Dinev, 2008) and positively influence government intrusion concerns (Dinev, 2008), behavioral intention to transact (Dinev and Hart, 2006b). Internet technical literacy was similarly shown to exert a negative impact on privacy concerns (Dinev and Hart, 2004; Brecht et al., 2012) and a positive impact on trust, readability of websites' privacy policy (Ermakova et al., 2014b) and privacy awareness (Brecht et al., 2012). Interestingly, actual Internet privacy literacy measured by a test provided opposite associations with privacy concerns and awareness (Brecht et al., 2012). Brecht et al. (2012) fur-

ther observed that stated Internet privacy literacy predominantly explained the variance in the content of privacy awareness.

Empirical studies indicated that social awareness exerted a positive impact on privacy concerns (Dinev and Hart, 2004, 2006b) and perceived need for government surveillance (Dinev 2008) and not significantly influenced government intrusion concerns (Dinev, 2008). Privacy awareness was similarly found to positively influence privacy concerns (Brecht et al., 2012; Ermakova et al., 2014a (NS)) as well as disposition to value privacy in the e-commerce, financial and healthcare fields (Xu et al., 2008). Related to social networking, the impact was not found to be significant. Technology awareness was shown to positively influence attitude towards behavior, behavioral intention (Dinev and Hu, 2005, 2007), and subjective norm (SN) (Dinev and Hu, 2007), and to be positively associated with PU, PEOU, perceived controllability (PC), and SE (Dinev and Hu, 2005). There are also some cultural moderating effects observed in the research. The relationships between awareness (A) and attitudes toward behavior (AB), and awareness (A) and behavioral intention (BI) to use antispyware were higher in the U.S. when compared to South Korea (Dinev et al., 2006b, 2009).

With regards to self-efficiency, Dinev and Hu (2005, 2007) do not find support for the hypothesis that SE influences perceived behavioral control, whereas Dinev et al. (2006b, 2009) do.

3. Cloud Computing in Healthcare

Title	Cloud Computing in Healthcare – a Literature Review on Current State of Research
Authors	Ermakova, Tatiana, Technical University of Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, tatiana.ermakova@tu-berlin.de Huenges, Jan, Technical University of Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, jan.huenges@ikm.tu-berlin.de Erek, Koray, Technical University of Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, koray.erek@tu-berlin.de Zarnekow, Rüdiger, Technical University of Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, ruediger.zarnekow@ikm.tu-berlin.de
Published in	Proceedings of the 19th Americas Conference on Information Systems (AMCIS 2013) (Ermakova et al., 2013b)
Abstract	Nowadays, IT resources are increasingly being used in all areas of the health sector. Cloud computing offers a promising approach to satisfy the IT needs in a favorable way. Despite numerous publications in the context of cloud computing in healthcare, there is no systematic review on current research so far. This paper addresses the gap and is aimed to identify the state of research and determine the potential areas of future research in the domain. We conduct a structured literature search based on an established framework. Through clustering of the research goals of the found papers we derive research topics including developing cloud-based applications, platforms or brokers, security and privacy mechanisms, and benefit assessments for the use of cloud computing in healthcare. We hence analyze current research results across the topics and deduce areas for future research, e.g., development, validation and improvement of proposed solutions, an evaluation framework.
Keywords	Cloud Computing, Healthcare, Literature Review

3.1 Introduction

Nowadays, IT resources are increasingly being applied in all health sector areas. They contribute to improving healthcare services, medical education and research (Nordin and Hassan, 2011; Nordin et al., 2012; Delgado, 2011). The new cloud computing technology promises to satisfy the IT needs in a more favorable way. Besides the many benefits cloud computing is known for (e.g., Mell and Grance, 2012), it is believed to open new healthcare specific perspectives (e.g., Chang et al., 2009; Chowdhary et al., 2011; Delgado, 2011; Loehr et al., 2010).

The literature covers the topic of cloud computing in healthcare from a variety of perspectives. Though there are numerous publications in the domain, we found no systematic review on current research so far. Based on these observations, we address this gap and derive the following research questions for our research:

(1) What are the main research topics in the context of cloud computing in healthcare?

(2) What are the current research findings on the identified research topics?

(3) What are potential areas of future research?

This research is aimed to support the TRESOR (TRusted Ecosystem for Standardized and Open cloud-based Resources) project (TRESOR, 2015) and conducted in accordance with the literature review frameworks proposed by vom Brocke et al. (2009), Webster and Watson (2002), and Cooper (1988). We systematically research articles published up to year 2012 in the context of cloud computing for healthcare and derive research topics by clustering the identified research goals. We present and discuss the current research results in accordance with the background of the papers, benefits and critical success factors seen by the authors for applying of cloud computing in healthcare, type of proposal, application area where applies and formulate the main ideas presented in the works. Finally, we summarize research potentials mentioned in the publications and conclude by our recommendations based on the literature review results and our interviews with multiple experts from the German healthcare industry.

The paper is structured as follows: We first define the scope of the review and conceptualize the topic. Next, we discuss the literature search process. We then analyze and synthesize the collected literature, present the current research issues and findings and derive a research agenda. Finally, we conclude by summarizing our results.

3.2 State of the Art Review on Cloud Computing in Healthcare

3.2.1 Definition of Review Scope

Defining the scope of the review we draw on an established taxonomy for literature reviews presented by Cooper (1988).

Characteristic		Categories			
(1)	Focus	Research outcomes	Research methods	Theories	Applications
(2)	Goal	Integration	Criticism	Identification of central issues	
(3)	Organization	Historical	Conceptual	Methodological	
(4)	Perspective	Neutral representation		Espousal of position	
(5)	Audience	Specialized scholars	General scholars	Practitioners	General public
(6)	Coverage	Exhaustive	Exhaustive and selective	Representative	Central / Pivotal

Table 4. Taxonomy of Literature Reviews (Following Cooper (1988))

Table 4 highlights the categories characterizing the present literature review. We focus (1) on research outcomes, research methods, theories, and applications. The goals (2) of our review include identifying central issues and integrating findings. For organizing (3) the review we apply a mix of historical, conceptual and methodological organizational formats. We take a neutral perspective (4) and hope to achieve results of value to general scholars as well as practitioners (5). We consider all the relevant sources, but describe only a meaningful sample (6).

3.2.2 Conceptualization of the Topic

Cloud computing with its Software (SaaS), Infrastructure (IaaS) and Platform (PaaS) as a Service delivery models represents a model providing on-demand access to a network-based cluster of shared computing resources and storage units (e.g., Mell and Grance, 2012; Foster et al., 2008) and promises numerous advantages over conventional in-house solutions (e.g., Tak et al., 2011). According to our analysis, most authors follow the definition of cloud computing proposed by Mell and Grance (2012) (Abbadi et al., 2011; Chen et al., 2012b; Delgado, 2011; Chen et al., 2012a). The second most often cited definition is proposed by Foster et al. (2008) (Chen et al., 2011; Nordin et al., 2011; Rolim et al., 2010).

3.2.3 Literature Search

We conduct the literature search process in accordance with the approach proposed by vom Brocke et al. (2009) in four phases, namely journal search, database search, keyword search and backward/forward search. We base on the AIS World MIS Journal Ranking for IS and Management literature to select journals and conferences. Aiming to ensure that all the journals and conferences are included we identify the EBSCOhost, IEEE Xplore, Emerald, ScienceDirect, AISeL, Springer, ACM Digital Library and Proquest databases. We derive the keywords from the key variables in the given context as well as their main synonyms, i.e. cloud, IaaS, SaaS, PaaS, and health, hospital, medical, and formulate the search phrases as all possible combinations of them. The results of the keyword search are shown in Table 5. A further combined backward and forward search leads us to 12 additional documents dealing with the topic.

Keywords / Database	cloud +			IaaS +			SaaS +			PaaS +			Sum Hits
	health	hospital	medical	health	hospital	medical	health	hospital	medical	health	hospital	medical	
EBSCOhost	924 (2)	288 (1)	626 (0)	17 (0)	2 (0)	10 (0)	109 (0)	37 (0)	48 (0)	18 (0)	5 (0)	21 (0)	2105 (3)
IEEE Xplore	250 (13)	67 (1)	436 (2)	7 (1)	2 (0)	7 (0)	16 (1)	8 (0)	21 (0)	5 (0)	3 (0)	6 (0)	828 (18)
Emerald	3 (0)	0 (0)	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	5 (0)
ScienceDirect	161 (0)	22 (0)	60 (1)	2 (0)	3 (0)	4 (0)	3 (0)	5 (0)	8 (0)	4 (0)	5 (0)	1 (0)	278 (1)
AISeL	27 (2)	1 (0)	12 (0)	0 (0)	0 (0)	0 (0)	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	42 (2)
Springer	96 (4)	15 (0)	61 (2)	3 (0)	3 (0)	1 (0)	3 (0)	1 (0)	1 (0)	1 (0)	0 (0)	0 (0)	185 (6)
ACM	30 (3)	4 (0)	22 (3)	1 (0)	14 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	71 (6)
Proquest	381 (0)	129 (0)	165 (0)	0 (0)	0 (0)	0 (0)	5 (0)	3 (0)	6 (0)	6 (0)	2 (0)	5 (0)	702 (0)
Sum Hits	1872 (24)	526 (2)	1384 (8)	30 (1)	24 (0)	22 (0)	138 (1)	54 (0)	84 (0)	34 (0)	15 (0)	33 (0)	4216 (36)

Table 5. Number of Found (and Relevant) Hits in the Keyword Search

3.2.4 Literature Analysis and Synthesis

Clustering the research goals of the found papers we derive the five main research areas, namely developing cloud-based applications, platforms or brokers, and security and privacy mechanisms, as well as assessing the benefits for the use of cloud computing in healthcare. We categorize the papers in accordance with the derived framework. We further evaluate the papers with respect to the background of the paper, benefits and critical success factors seen by the authors for applying of cloud computing in healthcare, kind of proposal, application area or methods used where applies and formulate the main ideas presented in the works. Here, we mostly rely on the description provided in the abstracts. To formulate the research agenda, we analyze the concluding parts of all papers with respect to the authors' suggestions for future research. We finally provide our own recommendations based on the literature review results and our interviews with the heads of IT departments, project managers and medical workers from different German hospitals.

3.3 Findings

3.3.1 Development of Cloud-Based Applications in Healthcare

The authors coming up with design proposals of cloud-based applications in healthcare refer to the limited access to patients' health data during medical service delivery (Poulymenopoulou et al., 2011; Kanagaraj and Sumathi, 2011; Karthikeyan and Sukanesh, 2012; Koufi et al., 2010; Rolim et al., 2010), the challenge of management and analysis of large data amounts (Huang et al., 2011), as well as high costs and waste of resources for constructing an independent information system (He et al., 2010; Kanagaraj and Sumathi, 2011). Cloud computing is expected to create a much more connecting environment for healthcare providers (Ratnam and Dominic, 2012), enable easy, immediate and ubiquitous access to health data (Poulymenopoulou et al., 2011; Koufi et al., 2010; Hoang and Chen, 2010), bring IT-related resources as services on demand (Karthikeyan and Sukanesh, 2012), while reducing costs (Deng et al., 2011; Hoang and Chen, 2010), providing scalability, high performance (Deng et al., 2011; Hoang and Chen, 2010), and being increasingly adopted among users (Hoang and Chen, 2010). The main barriers to the acceptance of cloud computing are seen in insufficient security and privacy protection (Deng et al., 2011; Hoang and Chen, 2010).

The contribution made by Rolim et al. (2010) delivers a telemedicine solution which integrates wireless sensor networks at a patient's bedside to automated data gathering and transmitting to an exchange service for further storage, processing and distribution to cloud services. Similar ideas are followed by Hoang and Chen (2010), Sharieh et al. (2012), and by Berndt et al. (2012) in the FEARLESS and eHealth-MV projects. In the model by Sharieh et al. (2012), the sensors are attached to the body to monitor oxygenated and deoxygenated hemoglobin concentration changes in the brain and tissues. In the MoCAsH (Mobile Cloud for Assistive Healthcare) infrastructure introduced by Hoang and Chen (2010), the collected data are further transmitted to the intelligent context-aware mobile cloud middleware. The authors additionally address scalability, load balancing, security and privacy in a federate cloud layer scheduling distributed clouds with respect to user security and resource requirements and guarantee the ease of service usage via a cloud portal.

The works presented by Koufi et al. (2010) and Poulymenopoulou et al. (2011) build an emergency medical system in a cloud environment on the basis of personal health records (PHRs) and other external systems. A further cloud-based emergency healthcare application proposed by Karthikeyan and Sukanesh (2012) uses palm vein pattern recognition technology for patient's identification and distributes an image processing tool, i.e. a DICOM (Digital Imaging and Communications in Medicine) viewer.

Deng et al. (2011) focus on home healthcare applications, particularly to support depressed patients, and introduce a cloud-based system design for home healthcare providing drug therapies, sleep and light, and physical activity management and other services. The authors derive security and privacy requirements applying business logic and architecture driven approaches, sketch out a plan to integrate the proposed architecture into a cloud, and give preliminary recommendations for health data protection. Home healthcare application scenarios can be also found in other works, e.g., by Abbadi et al. (2011), Deng et al. (2012), and Berndt et al. (2012). Deng et al. (2012) illustrate the home monitoring and wellbeing portal applications monitoring the patient's data uploaded via a mobile device to the cloud and sharing it with medical workers for further instructions on need or demand. Berndt et al. (2012) present the FEARLESS (Fear Elimination as Resolution for Loosing Elderly's Substantial Sorrows)

project to support elderly people in their self-serve activities by detecting a wide range of risks with a sensor (e.g., fall); the mobile diabetes (M-Diab) and mobile skin (M-Skin) systems to support the therapy and aftercare of patients suffering from diabetes and skin diseases, respectively; and the eHealth-MV (eHealth-Mecklenburg Vorpommern) project to estimate and monitor the stress and fitness level based on physiological signals gathered via wireless sensors.

He et al. (2010), Kanagaraj and Sumathi (2011) and Huang et al. (2011) propose cloud-based PACS (Picture Archiving and Communication System) to simplify the exchange of DICOM images between healthcare providers. Vazhenin (2012) presents the architecture of a cloud-based information retrieval service (e.g., DICOM) for a wide range of devices and provides performance measures of the implemented solution. The practical principles of constructing a cloud service can be found in the works by Zhang and Lu (2010), Chiang et al. (2011), and Ratnam and Dominic (2012).

3.3.2 Development of Cloud-Based Platforms in Healthcare

The authors of cloud-based platform designs for healthcare remark cloud computing as facilitating coordination among healthcare providers (Basu et al., 2012; Guo et al., 2010) and efficient use of medical resources (Guo et al., 2010), and enabling a broad set of healthcare scenarios (Chang et al., 2009). However, security and privacy are to be paid more attention to (Berndt et al., 2012; Ekonomou et al., 2011) as well as the related concerns of healthcare providers (Deng et al., 2012).

Chang et al. (2009) analyze cloud healthcare services based on the principles of sustainable ecological systems, deduce high-level requirements and provide an ecosystem analysis of several emerging healthcare ecosystems, e.g., radiology image data network, electronic medical/health record (EMR/EHR) and PHR ecosystems. Wang and Tan (2010) and Guo et al. (2010) consider a cloud-based platform to provide healthcare organizations with software services, a program development environment and hardware and computational resources. Ekonomou et al. (2011) elaborate on EHR and PHR integration in a cloud-based healthcare infrastructure. Berndt et al. (2012) derive basic functions of a SaaS platform. Basu et al. (2012) present a cloud-based Fusion platform sharing EHRs securely and aggregating de-identified data to support analytics applications, whereas Deng et al. (2012) introduce a trustworthy cloud platform provisioning healthcare services.

3.3.3 Development of Brokers for the Use of Cloud Computing in Healthcare

The proposals on the broker component are motivated by huge amount of medical resources to be handled (Nordin et al., 2011; Nordin and Hassan, 2011; Nordin et al., 2012). A broker is supposed to minimize user involvement in resources discovery (Nordin and Hassan, 2011) and composition (Wu and Khoury, 2012) ensuring the quality of services and the satisfaction of a user's need (Nordin et al., 2012). It is expected to particularly forward the exchange of medical records between different healthcare providers (Wu and Khoury, 2012; Nordin et al., 2012; Nordin et al., 2011; Nordin and Hassan, 2011) by discovering and selecting correct (Nordin et al., 2012; Nordin et al., 2011; Nordin and Hassan, 2011) as well as complete and unique (Wu and Khoury, 2012) medical records and optimizing the response time when retrieving the data from the distributed database repository (Nordin and Hassan, 2011). In general, the authors believe to minimize the treatment delay (Nordin et al., 2012; Nordin and Hassan, 2011) and reduce medical errors and cost (Wu and Khoury, 2012). The studies on the

broker cover goal-based (Nordin and Hassan, 2011; Nordin et al., 2011), agent-based (Nordin et al., 2012) and workflow- and QoS-based brokers (Wu and Khoury, 2012).

3.3.4 Development of Security and Privacy Mechanisms for the Use of Cloud Computing in Healthcare

The well-known benefits of cloud computing as cost reduction (Loehr et al., 2010; Chen et al., 2012a), metered and flexible utilization of its resources (Chen and Hoang, 2011; Chen et al., 2012a; Li et al., 2011a; Li et al., 2010) are also being seen as advantages with respect to health information systems. Receiving increasing adoption among users (Chen and Hoang, 2011), cloud computing is characterized here as enabling one storage center for health data (Li et al., 2011b; Shini et al., 2012) and increased-volume and open collaboration between physicians (Shini et al., 2012), enhancing the availability, recovery and transfer of health records (Nematzadeh and Camp, 2010), providing easy and ubiquitous access to health data (Loehr et al., 2010; Chen and Hoang, 2011; Chen et al., 2012a) and massive storage space (Shini et al., 2012), improving and enhancing medical services and creating new business models opportunities in healthcare (Loehr et al., 2010).

Nevertheless, cloud computing also faces many security and privacy challenges, which raise wide concerns among patients and medical workers (Li et al., 2011b; Li et al., 2012; Chen et al., 2012a; Deng et al., 2012; Shini et al., 2012; Abbadi et al., 2011), in particular the risk of losing control over data (Chen and Hoang, 2011; Li et al., 2010).

Zhang and Liu (2010), Abbadi et al. (2011), and Shini et al. (2012) derive security and privacy requirements and techniques for sharing of medical data in the cloud. Similarly, security and privacy challenges are identified and addressed by Loehr et al. (2010) introducing a security e-health infrastructure based on Trusted Virtual Domains, Nematzadeh and Camp (2010) designing a traitor-tracing algorithm, Deng et al. (2011) establishing trustworthy middleware services, Li et al. (2011a) elaborating on unlinkability between the patient and the electronic health record, Li et al. (2011b) defining a keyword search framework over encrypted records, and Li et al. (2010), Yu et al. (2010), Chen and Hoang (2011), Basu et al. (2012), Chen et al. (2012a), Chen et al. (2012b), Li et al. (2012) proposing novel access control mechanisms.

3.3.5 Potentials and Challenges for the Use of Cloud Computing in Healthcare

Though being in the very early development phase (Chowdhary et al., 2011), cloud computing is seen as increasing existing capacities or adding new ones without additional resource expenditures (Chowdhary et al., 2011; Delgado, 2011). In particular, it delivers ubiquitous access to platforms and services (Chowdhary et al., 2011; Fernández-Cardeñosa et al., 2012).

Osterhaus (2010) and Sarnikar (2011) elaborate on the potential usage of cloud computing in healthcare and provide guidelines for decision making. Mohammed und Fiaidhi (2010) discuss the ubiquity notion in sharing EHRs through the cloud computing paradigm and related security concerns, being also addressed by Delgado (2011). Chowdhary et al. (2011) examine the application of cloud computing for e-health and deduce capacity building, observatory on the latest research information and tools, and interoperability using universal standards as future prospects. Fernández-Cardeñosa et al. (2012) analyze the usage of an EHR management system for a large hospital and a network of primary healthcare centers and derive the feasibility of a hybrid solution implying the storage of the EHRs with images in hospital serv-

ers and the rest in the cloud. The experiments by Huang et al. (2011) show a six time improvement of the throughput of the initial model through the usage of cloud computing.

3.4 Research Agenda

Many authors express the intention to extend their current work further (Abbadi et al., 2011; Berndt et al., 2012; Chowdhary et al., 2011; Hoang and Chen, 2010; Huang et al., 2011; Nordin et al., 2011; Nordin et al., 2012; Karthikeyan and Sukanesh, 2012; Li et al., 2010; Loehr et al., 2010; Poulymenopoulou et al., 2011).

In the security and privacy area, the future research potential is observed in further development and improvement of the existing mechanisms (Abbadi et al., 2011; Deng et al., 2011; Shini et al., 2012; Loehr et al., 2010) and establishing human trust through campaigns (Ekonomou et al., 2011).

Furthermore, the research findings are going to be deployed in real world settings (Abbadi et al., 2011; Deng et al., 2011; Ekonomou et al., 2011; Hoang and Chen, 2010; Nematzadeh and Camp, 2010; Poulymenopoulou et al., 2011; Rolim et al., 2010), to be simulated (Nordin and Hassan, 2011) or extended to mobile cloud (Karthikeyan and Sukanesh, 2012).

Following Rolim et al. (2010), there is a research potential in the validation of the proposed solutions in the real word settings with respect to scale and security enhancement. Koufi et al. (2010) point out the usability criterion for system evaluation. Sharieh et al. (2012) are interested in the performance and data integrity results in the case of transmission of different data types.

From our perspective, there is also a lack of a measurement framework to evaluate the proposals (e.g., performance (Nordin et al., 2012; Sharieh et al., 2012), efficiency, users' acceptance, etc.) and, following the expert interviews, an overview of potential application scenarios and typical requirement patterns systematically derived, business and actor models for an ecosystem.

3.5 Conclusion

The literature review shows that the application of the cloud computing paradigm in healthcare is heavily discussed. The literature search process reveals 36 articles in this area across the main databases covering top-ranked IS and Management journals and conference proceedings and 12 additional ones through the backward/forward search.

We observe research proposals for various application fields including emergency healthcare, home healthcare, assistive healthcare, and telemedicine, as well as storage, sharing and processing of large medical resources (e.g., images) in general. Gaining popularity among users, cloud computing is believed to improve accessibility of health data, ensure efficient management and usage of medical resources, facilitate collaboration among healthcare organizations, and open new possibilities for healthcare. However, security and privacy still remain the main concerns. Further research potential is observed in the security and privacy area, the proposals' development, simulation in the real world settings and extension to mobile computing. We observe research needs in a measurement framework to evaluate the proposals, and, based

on the interviews with German healthcare experts, an overview of potential application scenarios, typical requirement patterns systematically derived, business and actor models for an ecosystem.

4. Investigating Acceptance of Health Clouds

Title	Acceptance of Health Clouds – A Privacy Calculus Perspective
Authors	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
Published in	Proceedings of the 22th European Conference on Information Systems (ECIS 2014) (Ermakova et al., 2014a)
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

4.1 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, 2015), 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, 2006a; 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.

4.2 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 R2 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, 2006a; 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.

4.2.1 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).

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 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.

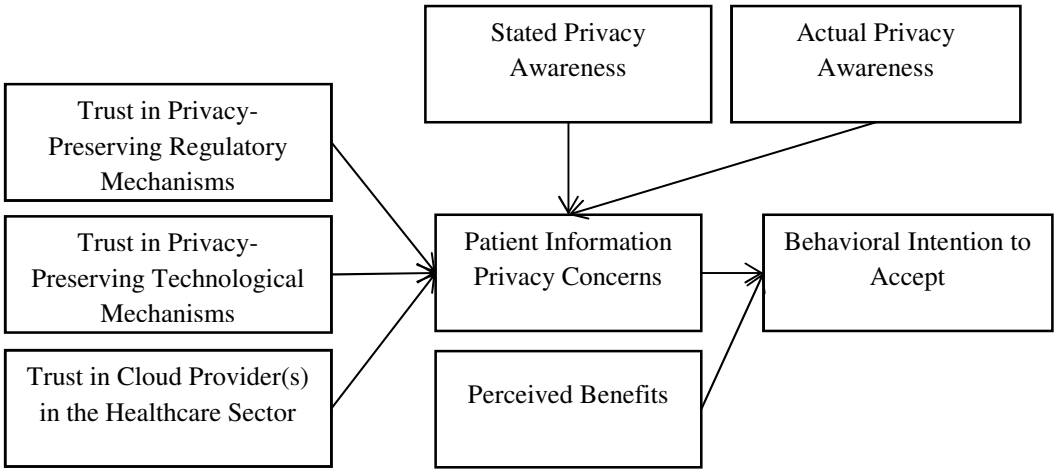

Figure 4. Research Model

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.

4.3 Model Construction and Instrument Development

Our hypothesized model drawn from the theoretical foundations in Section 4.2 is presented in Figure 4 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.

In Table 6, 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**
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 (2006a))
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 6. Research Model Constructs and Related Questionnaire Items (Part 1)

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 (2006a), 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 7. Research Model Constructs and Related Questionnaire Items (Part 2)

4.4 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 8. 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 9. 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.

4.5 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.

4.5.1 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 10. 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 11. Item Loadings and Cross-Loadings (Part 2)

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 10). 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 12).

	AVE	CR	R2	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 12. Internal Consistency and Discriminant Validity of Constructs (CR = Composite Reliability, CA = Cronbachs Alpha)

Following the recommendations by Chin (1998), we examine discriminant validity by checking whether all the loadings are higher than cross-loadings (see Table 10) and the square roots of the AVE of the construct are higher than the correlation between the construct and any other construct (see Table 12). 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. Table 10, Table 12 and Table 13 present the final results of our model testing.

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

4.5.2 Structural Model

The results of our structural model testing are presented in Table 13. 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 infor-

mation privacy awareness, both stated and actual, in building their patient information privacy concerns.

4.6 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.

5. Security and Privacy Requirements for Health Clouds

Title	Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios
Authors	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
Published in	Proceedings of the 19th Americas Conference on Information Systems (AMCIS 2013) (Ermakova et al., 2013b)
Abstract	The emerging cloud computing technology enables new essential scenarios in healthcare, in particular those of data sharing among practitioners. Nevertheless, their security and privacy concerns still impede the wide adoption of cloud computing in this area. Although there are numerous publications in the context of cloud computing in healthcare, we found no consistent typical security and privacy system requirements framework in this domain so far. Owing to the lack of those studies and preparing the ground for creating secure and privacy-friendly cloud architectures for healthcare, we survey security and privacy system requirements for cloud-based medical data sharing scenarios using two strategies. We base on a systematic design science approach following the literature-driven requirement elicitation strategy and apply an established security requirement elicitation methodology as part of the scenario-driven strategy. Finally, we evaluate and compare the two security and privacy system requirements elicitation strategies used in this paper.
Keywords	Cloud Computing, Healthcare, Security, Privacy, Requirement

5.1 Introduction

There are multiple new scenarios enabled through the adoption of the emerging cloud computing technology in healthcare (Loehr et al., 2010), whereas the data sharing scenarios are of high relevance to practitioners (He et al., 2010; Kanagaraj and Sumathi, 2011; Huang et al., 2011; Zhang and Lu, 2010). Nevertheless, cloud computing also faces many security and privacy challenges (Deng et al., 2011; Ekonomou et al., 2011), which raise wide concerns among patients and medical workers (Li et al., 2011b; Li et al., 2012; Chen et al., 2012a; Deng et al., 2012; Shini et al., 2012; Abbadi et al., 2011), in particular the risk of losing control over data (Chen and Hoang, 2011; Li et al., 2010). Many researchers observe a research potential with respect to the existing security and privacy preserving mechanisms (Loehr et al., 2010; Abbadi et al., 2011; Deng et al., 2011; Shini et al., 2012), while Ekonomou et al. (2011) call for establishing human trust campaigns.

Although there are numerous publications in the domain of cloud computing in healthcare, to our knowledge there are few works about general and systematic security and privacy system requirements frameworks so far (Zhang and Liu, 2010; Deng et al., 2011) and none that are elicited by multilateral requirements engineering methods, which would be able to also point out potential conflicts between the requirements. With this background we aim to take first steps to close this research gap.

The present work is aimed to support the TRESOR (TRusted Ecosystem for Standardized and Open cloud-based Resources) research project with healthcare practitioners (TRESOR, 2015) funded by the German Federal Ministry of Economics and Technology. To elicit security and privacy system requirements, we follow literature-driven and scenario-driven strategies. The implication of the first strategy is conducted in accordance with the design science framework proposed by Hevner et al. (2004). Based on the literature search framework introduced by vom Brocke et al. (2009), we systematically review articles published up to year 2012 dealing with security and privacy preserving mechanisms for the use of cloud computing in healthcare, then define system security and privacy requirements, and evaluate them in semi-structured interviews with different experts from the German healthcare industry. We use the requirement pattern presented by Rupp (2005, in German) to formulate the requirements. The second strategy covers security and privacy system requirements arising from specific processes and multiple stakeholders with different interests in healthcare data sharing scenarios and relies on an established security requirements elicitation methodology called Multilateral Security Requirements Analysis (MSRA) (Fabian et al., 2010; Gürses et al., 2005; Gürses and Santen, 2006; Gürses et al., 2006; Gürses, 2010). Finally, we provide a comparison of the two security and privacy elicitation strategies and further research options in this field.

The paper is organized as follows. The background and work related to the topic is provided in section 5.2. We introduce our research design in section 5.3 and present the results in the 5.4th section. In conclusion, we summarize all findings and present our further research directions.

5.2 Background and Related Work

The relatively new technology of cloud computing creates a scenario diversity in healthcare (Loehr et al., 2010), one of them the medical data sharing scenarios remarked by He et al. (2010), Kanagaraj and Sumathi (2011), Huang et al. (2011), and Zhang and Lu (2010) as be-

ing of particularly high relevance to practitioners. The wide adoption of cloud computing in healthcare is, however, impeded by many still open security and privacy challenges (Deng et al., 2011; Ekonomou et al., 2011). Li et al. (2011b), Li et al. (2012), Chen et al. (2012a), Deng et al. (2012), Shini et al. (2012), Abbadi et al. (2011) speak about concerns among patients and medical workers, which Chen and Hoang (2011) and Li et al. (2010) in particular relate to the risk of losing control over data. Loehr et al. (2010), Abbadi et al. (2011), Deng et al. (2011), and Shini et al. (2012) call for further research on the existing security and privacy preserving mechanisms, while Ekonomou et al. (2011) propose undertaking campaigns for establishing human trust.

An unsystematic analysis of some related security and privacy threats for medical data sharing scenarios in the cloud computing environment is provided by Nematzadeh and Camp (2010), Shini et al. (2012), and Loehr et al. (2010). There are also some authors who introduce security and privacy-enhancing mechanisms, however without a careful analysis of multilateral security and privacy requirements. Those works elaborate on access control (Basu et al., 2012; Chen and Hoang, 2011; Chen et al., 2012a; Chen et al., 2012b; Li et al., 2010; Li et al., 2012; Yu et al. 2010), keyword search over encrypted records (Li et al., 2011b), unlinkability between the patient and the electronic health record (Li et al., 2011a), and tracing of traitors (Nematzadeh and Camp, 2010). Attempts to elicit security and privacy system requirements with respect to medical data sharing in the cloud were undertaken by Zhang and Liu (2010) and Deng et al. (2011). Deng et al. (2011) relied on the business logic and the architecture of a home healthcare system in the cloud, particularly aimed to support depressed patients. The review of related literature thus shows there is no security and privacy system requirements framework elicited by established security requirement elicitation approaches (Gürses et al., 2005; Gürses and Santen, 2006; Gürses et al., 2006; Gürses, 2010; Fabian et al., 2010), in particular the multilateral ones, which would be able to also point out potential conflicts between requirements.

5.3 Research Design

In our research, we apply literature-driven and scenario-driven strategies to elicit security and privacy requirements.

While applying the first one, we follow the design science framework proposed by Hevner et al. (2004) and elicit system requirements in three cycles, namely rigor cycle, design cycle, relevance cycle. In the rigor cycle, we conduct a systematic literature search on security and privacy friendly mechanisms for the use of cloud computing in healthcare in accordance with the literature search framework proposed by vom Brocke et al. (2009). We base on the AIS ranking list and search in the EBSCOhost, IEEE Xplore, Emerald, ScienceDirect, AISeL, Springer, ACM Digital Library and Proquest literature databases, and apply a combined backward and forward search. Then we evaluate the findings of the literature analysis and define the initial draft in the design cycle. In the final relevance cycle we conduct semi-structured interviews with different experts from the German healthcare industry to evaluate the developed requirements. We formulate the requirements in accordance with the framework presented by Rupp (2005, in German).

To define scenario-driven, multilateral security and privacy requirements, we follow the multilateral security requirements analysis (MSRA) method (Gürses et al., 2005; Gürses and Santen, 2006; Gürses et al., 2006; Gürses, 2010; Fabian et al., 2010). According to Fabian et al. (2010), the paradigm of multilateral security contradicts the traditional view by acknowledg-

ing stakeholders' conflicting interests with respect to assets. This is essential in healthcare delivery involving multiple parties. Based on the main functionalities of a data sharing scenario enabled through cloud computing, we identify stakeholders, i.e., parties concerned to the system-to-be, and elaborate on their security and privacy goals. In all the steps, we rely on the expert interviews and the literature analysis. In our further research we are going to identify facts and assumptions as the relevant properties of the environment and refine stakeholder views on the scenario taking them into account, reconcile the identified security and privacy goals by capturing conflicts between them, finding compromises between conflicting goals, and establishing a consistent set of security and privacy system requirements. Finally, we will reconcile them and functional requirements in a real project.

5.4 Results

5.4.1 Literature-Driven System Security and Privacy Requirements Collection

Type	Concept / Security or Privacy Goal	Source	Requirement
Security	Users' Authenticity and Authentication	Zhang and Liu (2010), Chen et al. (2012a), Chen et al. (2012b)	The system shall verify the identities of users at the entry of every access (Zhang and Liu, 2010).
Security	Non-Repudiation of Users' Actions	Zhang and Liu (2010), Chen et al. (2012a), Chen et al. (2012b)	The system shall ensure that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction (Zhang and Liu, 2010).
Security	Non-Repudiation of Users' Emergency Access	Loehr et al. (2010)	The system shall ensure that one cannot deny having had an emergency access.
Security	Auditability of Users' Actions	Zhang and Liu (2010), Chen and Hoang (2011), Deng et al. (2011), Basu et al. (2012), Chen et al. (2012b)	The system shall record user actions (e.g., in a chronological order by maintaining a log of every access to and modification of data) (Zhang and Liu, 2010).
Security	Users' Sharing and Access without Patient's Involvement	Loehr et al. (2010), Basu et al. (2012)	The system shall enable data sharing and access without the patient's involvement.
Privacy	Users' Anonymity	Loehr et al. (2010), Nematzadeh and Camp (2010), Li et al. (2011b)	The system shall prevent determining the user's identity based on her actions and/or indexes (Li et al. 2011b).
Privacy	Confidentiality of Users' Access Privileges	Chen and Hoang (2011), Yu et al. (2010)	The system shall ensure access privileges information is accessible only to the authorized users.

Table 14. User-Related System Security and Privacy Requirements Collection through a Literature Analysis

Zhang and Liu (2010) refer to traditional security goals (e.g., Fabian et al., 2010) confidentiality, integrity and availability extended by authentication, non-repudiation, and audit and ar-

chiving, as well as ownership of information, patent consent and authorization. These are referred to and used by Chen et al. (2012b) and further extended by Deng et al. (2011).

Type	Concept / Security or Privacy Goal	Source	Requirement
Security	Ownership of Medical Record	Zhang and Liu (2010), Chen et al. (2012b), Shini et al. (2012)	The system shall define the creator, author and manager of the data (Zhang and Liu, 2010).
Security	Confidentiality of Medical Record	Zhang and Liu (2010), Yu et al. (2010), Chen and Hoang (2011), Deng et al. (2011), Li et al. (2011a), Basu et al. (2012), Chen et al. (2012b), Li et al. (2012), Shini et al. (2012)	The system shall ensure the data is accessible only to the authorized readers (Zhang and Liu). The system shall ensure the data is accessible only to the unauthorized contributors (Li et al., 2012).
Security	Integrity of Medical Record	Zhang and Liu (2010), Chen and Hoang (2011), Deng et al. (2011), Li et al. (2011a), Chen et al. (2012a), Chen et al. (2012b), Shini et al. (2012)	The system shall preserve the accuracy and consistency of data (Zhang and Liu, 2010).
Security	Availability and Utility of Medical Record	Deng et al. (2011), Basu et al. (2012), Shini et al. (2012)	The system shall ensure the availability and utility of data when needed.
Security	Archiving of Medical Record	Zhang and Liu (2010), Chen et al. (2012b)	The system shall restore data without a loss when needed (Zhang and Liu, 2010).
Security	Patient Consent and Authorization for Medical Record Sharing	Zhang and Liu (2010), Deng et al. (2011), Chen et al. (2012b), Basu et al. (2012)	The system shall allow the patient to grant rights over her or his data to other users (Zhang and Liu, 2010).
Security	Fine-Grained Access to Medical Record	Li et al. (2010), Yu et al. (2010), Chen and Hoang (2011), Deng et al. (2011), Li et al. (2011b), Basu et al. (2012), Li et al. (2012)	The system shall ensure different users are authorized to read and write different sets of data (Li et al., 2010; Li et al., 2012; Li et al., 2011b).
Security	Revocation of Access to Medical Record	Li et al. (2010), Li et al. (2011b), Basu et al. (2012), Li et al. (2012)	The system shall prevent the user from future access when necessary (Li et al., 2010; Li et al., 2012; Li et al., 2011b). The system shall prevent the user from access to future data when necessary (Li et al., 2012).

Table 15. Medical Record-Related System Security and Privacy Requirements Collection through a Literature Analysis (Part 1)

The special properties addressed by the authors of security and privacy friendly mechanisms for the use of cloud computing in healthcare data sharing scenarios are formulated as fine-grained access control (Li et al., 2010; Yu et al., 2010; Chen and Hoang, 2011; Li et al., 2011b; Basu et al., 2012; Li et al., 2012), access right revocation (Li et al., 2010; Li et al., 2011b; Li et al., 2012; Basu et al., 2012), flexible data access policies (especially under emergency scenarios) or emergency exceptions (Li et al., 2010; Li et al., 2011a; Li et al., 2012), efficiency, scalability, and usability (e.g., user secret key accountability) of the proposed

mechanisms (Li et al., 2010; Yu et al., 2010; Li et al., 2011b; Basu et al., 2012; Li et al., 2012), write access control (Li et al., 2012), record anonymity (Li et al., 2011a), index and query privacy (Li et al., 2011b), and user access privilege confidentiality (Yu et al., 2010). Further related concepts include prevention of security attacks and violations (Nematzadeh and Camp, 2010; Chen et al., 2012b; Shini et al., 2012), data sharing and access without the patient's involvement (Loehr et al., 2010; Basu et al., 2012), secure record's navigation (Basu et al., 2012), confidentiality of a medical record's existence for a given person (Loehr et al., 2010), client anonymity (Loehr et al., 2010; Nematzadeh and Camp, 2010), and non-repudiation of emergency access (Loehr et al., 2010).

Type	**Concept / Security or Privacy Goal**	**Source**	**Requirement**
Security	Flexible or/and Emergency Access to Medical Record	Li et al. (2010), Nematzadeh and Camp (2010), Deng et al. (2011), Li et al. (2011a), Li et al. (2012)	The system shall allow changes to the data access policies (Li et al., 2010; Li et al., 2012).
Privacy	Unlinkability between Patients and Medical Records	Li et al. (2011a)	The system shall ensure the unlinkability between patients and documents (Li et al., 2011a).
Privacy	Patients' Anonymity in Medical Record	Deng et al. (2011)	The system shall prevent determining the patient's or/and owner's identity based on the document (Li et al., 2011a).
Privacy	Confidentiality of Medical Record's Existence	Loehr et al. (2010), Basu et al. (2012)	The system shall ensure information about a document's existence for a given patient is accessible only to the authorized users (Loehr et al., 2010).

Table 16. Data-Related System Security and Privacy Requirements Collection through a Literature Analysis (Part 2)

Type	**Concept / Security or Privacy Goal**	**Source**	**Requirement**
Security	Availability and Utility of System	Zhang and Liu (2010), Deng et al. (2011), Chen et al. (2012b)	The system shall serve its purpose and be available when needed (Zhang and Liu, 2010).
Security	Efficiency, Scalability and Usability of System	Li et al. (2010), Yu et al. (2010), Deng et al. (2011), Li et al. (2011b), Basu et al. (2012), Li et al. (2012)	The system shall be efficient, scalable and usable. The system shall support a large and unpredictable number of users (Li et al., 2010; Li et al., 2012; Li et al. 2011b).
Security	Detection and Prevention of Security Attacks and Violations in System	Nematzadeh and Camp (2010), Chen and Hoang (2011), Chen et al. (2012b), Shini et al. (2012)	The system shall detect and prevent any security attacks and violations (e.g., illegal behavior over data) (Chen and Hoang, 2011), e.g. by sending an alert when malicious action is in progress.

Table 17. System-Related System Security and Privacy Requirements Collection through a Literature Analysis

Based on these observations, we derive three system security and privacy requirements collection sets, namely those directly related to users, i.e., medical workers, the flow and storage of

medical records and the system itself, which we respectively present in Table 14, Table 15, and Table 17. An initial observation already reveals some conflicts between the security and privacy goals specified, e.g., patent consent and authorization to medical record sharing and users' sharing and access without the patient's involvement, auditability of users' actions and users' anonymity, as well as confidentiality of medical records and emergency exception. This supports the necessity of a multilateral security paradigm.

5.4.2 Scenario Driven Security and Privacy Requirements Elicitation

Following the MSRA framework provided by TAPAS (2004), Gürses et al. (2005), and Fabian et al. (2010) and based on the preliminary literature analysis and expert interviews, we identify direct stakeholders whose information is being exchanged and indirect stakeholders only interested in the system-to-be. The information exchanged is then specified in an information model.

Stakeholder	Information Object	Counter-Stakeholder	Requirement Derived from a Literature Analysis
Patient	Medical Records	Clinician	Confidentiality of Medical Record Integrity of Medical Record Fine-Grained Access to Medical Record Revocation of Access to Medical Record Flexible or/and Emergency Access to Medical Record Patient Consent and Authorization to Medical Data Sharing
		Non-Clinician	Confidentiality of Medical Record's Existence Unlinkability between Patients and Medical Records
	Identification Data	Non-Clinician	Patients' Anonymity in Medical Record
	Patients' Data (possibly) to be revealed from Clinicians' Actions and/or Indexes	Non-Clinician	
Clinician	Actions and Identification Data	Outside	Users' Anonymity
	Access Privileges	Outside	Confidentiality of Users' Access Privileges
	Decisions (possibly) to be revealed from Medical Records	Non-Clinician	
	Local Content	Outside	

Table 18. System Security and Privacy Requirements Collection through a Scenario Analysis

In the taxonomy of direct stakeholders' roles, we differentiate between the roles of Patient and Clinician who may be a doctor (e.g., intern, senior physician, chief physician, and consultant physician) or a nurse (e.g., nurse, senior nurse, and medical registration). Among indirect stakeholders, we distinguish between a Health Care Cloud (HCC), some independent researcher, the government, Healthcare Certification Authority (HCA), National Health Insurance (NHI) (TAPAS, 2004; Li et al., 2011a) and a non-clinician in a healthcare organization

who may perform QA (Quality Assurance) management, administration (e.g., administrative employee, administrative registration, research employee, controlling, data protection officer), IT-administration, or spiritual welfare.

A scenario where information sharing between clinicians with respect to a patient takes place can be described as follows. After completion of treatment, the patient is discharged from the hospital and goes to another hospital or rehabilitation facility. Her doctor sends medical records containing the patients' medical history, diagnosis, medications, allergies etc., whereas the nurse provides other information, e.g., the patient's having an infectious germ. The communication is enabled via cloud. Similar information sharing scenarios are considered in the works by He et al. (2010), Kanagaraj and Sumathi (2011), Huang et al. (2011), Zhang and Lu (2010).

For our main two direct stakeholders' roles, we formulate corresponding information models. The information being shared about a Patient includes:

- medical records;
- patients' identification data (possibly) contained in medical records;
- patients' data (possibly) to be revealed from clinicians' actions and/or indexes.

The information model of a Clinician constitutes:

- clinicians' actions (e.g., data transmission or/and reception) and identification data audited for non-repudiation purposes;
- clinicians' access privileges;
- clinicians' decisions (possibly) to be revealed from medical records;
- local content in case of using local-based services.

Potential security threats may arise from both inside and outside counter-stakeholders driven by curiosity, the expectation of profit making, etc. (TAPAS, 2004; Deng et al., 2011). The potential counter-stakeholders can be other patients, medical personal not involved in the treatment, colleagues of the patient, insurance companies, the public, etc.

In Table 18, we define some requirements suggestions describing which counter-stakeholder's actions should be restricted in respect to which information object of which stakeholder and compare them to the previously derived ones. The possible actions here may include sharing, reading, modifying, and deleting. The table shows, the requirement sets derived through a literature and scenario analysis have many requirements in common as well as contain some unique ones.

5.5 Conclusion and Further Work

The wide adoption of the new cloud computing paradigm facilitating new essential scenarios in healthcare is mainly restricted by security and privacy challenges and concerns.

In the present work, we derived a set of security and privacy system requirements for adopting cloud computing in healthcare data sharing scenarios based on a design science approach in the literature-driven strategy and the multilateral security requirements analysis methodology in the scenario-driven strategy.

Both requirements elicitation strategies gave many common results, but also helped to capture some unique requirements, thus supplementing each other. The common requirements are related to the medical records and identification data of patients, as well as the actions, identification data, and access privileges of clinicians in the system. The scenario analysis also revealed patients' data (possibly) to be revealed from clinicians' actions and/or indexes, decisions (possibly) to be revealed from medical records, and local content in case of using local-based services as protection targets. The literature analysis additionally pointed out users' authenticity and authentication; auditability, non-repudiation of users' emergency and non-emergency actions; users' actions with and without patient's involvement; as well as system's availability and utility, efficiency, scalability and usability, and detection and prevention of security attacks and violations there. Thus, the comparison shows, the scenario-driven strategy provides much more detailed results, whereas the literature-driven strategy gives a more comprehensive varied requirements set, here possibly due to mature state of research in this field.

The observation of the results of the adoption of the literature-derived strategy revealed some conflicts between the security and privacy goals specified, e.g., patent consent and authorization to medical record sharing and user's sharing and access without the patient's involvement, auditability of users' actions and users' anonymity, as well as confidentiality of medical records and emergency exception. Through the application of the principles of the established MSRA method in the information sharing scenario, we identified the concerned parties and their security and privacy information assets to be protected. Our future work here will be aimed at identifying facts and assumptions and refining stakeholder views, capturing conflicts between security and privacy goals and searching compromises between them to make the security and privacy requirements set consistent.

The concluding research goal we see is a more detailed evaluation and comparison of the two security and privacy elicitation techniques used in this paper, namely the literature research focusing on system security and privacy system requirements within a design science framework, and an established multilateral security requirements method that is able to refine the former approach and to point out (and hopefully solve) potential requirements interactions or conflicts in an early system development phase.

6. Security and Privacy-Preserving Architecture for Health Clouds

Title	Secret Sharing for Health Data in Multi-Provider Clouds
Authors	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
Published in	Proceedings of the 15th IEEE Conference on Business Informatics (IEEE CBI 2013) (Ermakova and Fabian, 2013)
Abstract	The accelerated adoption of cloud computing among enterprises is due to the multiple benefits the technology provides, one of them the simplification of inter-organizational information sharing, which is of utmost importance in healthcare. Nevertheless, moving sensitive health records to the cloud still implies severe security and privacy risks. With this background, we present a novel secure architecture for sharing electronic health records in a cloud environment. We first conducted a systematic literature review and interviews with different experts from the German healthcare industry that allowed us to derive real-world processes and corresponding security and privacy requirements. Based on these results, we designed our multi-provider cloud architecture that satisfies many of the requirements by providing increased availability, confidentiality and integrity of the medical records stored in the cloud. This architecture features secret sharing as an important measure to distribute health records as fragments to different cloud services, which can provide higher redundancy and additional security and privacy protection in the case of key compromise, broken encryption algorithms or their insecure implementation. Finally, we evaluate and select a secret-sharing algorithm for our multi-cloud architecture. We implemented both Shamir's secret-sharing scheme and Rabin's information dispersal algorithm and performed several experiments measuring the execution time. Our results indicate that an adoption of Rabin's algorithm would create a low overhead, giving strong indicators to the feasibility of our approach.
Keywords	Electronic Health Record, Cloud Computing, Security, Secret-Sharing Scheme

6.1 Introduction

Known for multiple benefits, cloud computing is increasingly being adopted among enterprises. The relatively new technology can simplify information sharing among different business partners, which is also of utmost importance in healthcare.

Nowadays, the exchange of medical records between healthcare providers can still be very conventional and impractical in practice. Moreover, physical medical records that are shared between hospitals may include patient identifiers and highly sensitive information. If they are transmitted in a casual way, privacy of the patient can be violated.

Electronic health records (EHR) in a cloud-computing environment have been attracting extensive attention from both academia and practitioners. Following Loehr et al. (2010), we define an EHR as a subset of electronic medical record shared across health centers (HC) by medical workers. The cloud computing approach does not just provide adequate data storage capacities (Li et al., 2011b; Shini et al., 2012) and facilitate storing of health data in one centralized place (Li et al., 2011b). It is also characterized as enhancing the transfer, availability and recovery of health records (Nematzadeh and Camp, 2010), providing an easy and ubiquitous access to health data (Loehr et al., 2010; Bessani et al., 2011; Chen et al., 2012a), improving and enhancing medical services, opening new business models opportunities (Loehr et al., 2010) as well as receiving an increasing adoption by users (Bessani et al., 2011). The well-known benefits of cloud computing such as cost reduction (Loehr et al., 2010; Chen et al., 2012a), metered and flexible utilization of its resources (Bessani et al., 2011; Chen et al., 2012a; Li et al., 2011a; Li et al., 2010) are also often mentioned with respect to health record systems.

Nevertheless, the new promising cloud computing paradigm also faces many security and privacy challenges, which raise wide concerns among patients and medical workers (Li et al., 2011b, 2012; Chen et al., 2012a), in particular the risk of losing control over data (Bessani et al., 2011; Li et al., 2010). There are multiple approaches in the literature, which discuss corresponding data security and privacy protection issues and present novel encryption algorithms to mitigate some of the problems (see Section 6.2). However, few of these approaches so far take the risk of key compromise into account. If an EHR is stored in an encrypted format at a cloud provider (CP), but the decryption key is compromised at any time in the future, the provider could have full access to the sensitive patient data. Flawed encryption algorithms and error-prone implementations pose similar risks. Based on these observations, we investigate security and privacy requirements and corresponding mechanisms.

This paper presents a novel architecture for sharing electronic health records in a multi-cloud environment, i.e., where data is not only stored at a single CP, but at several independent providers in parallel. Our architecture satisfies many of the requirements derived from expert interviews during an ongoing case study and a thorough literature analysis. The main features provided by our system include increased data availability, confidentiality and integrity of the documents stored in the cloud, the unlinkability between the medical records and patients, confidentiality of identifiers and of the existence of a medical record for a given patient against external parties.

Our approach is in particular based on secret sharing, where we apply the scheme proposed by Shamir (1979) to split the encrypted EHR into shares that are stored at different CPs. In comparison to the recent developments on data partitioning and dispatching across multiple CPs

(e.g., Liu et al. (2012)), this method guarantees the exact document recovery in the presence of at least t shares (t is a parameter that can be chosen freely, but should be public), and perfect secrecy in all other cases. We publish each share to a different CP. This means that as long as fewer than t cloud providers collude to break patient privacy, they cannot reconstruct the EHR, even if they should be able to break its encryption. Moreover, this provides data redundancy for increased availability: some shares can get lost without preventing the reconstruction by authorized entities.

During this procedure, we use the cryptographic hash of (the concatenation of) document and share identifiers as search key, in order to obfuscate any sensitive identifiers in document names. This also prevents linkability of shares by their names in case of provider collusion.

We additionally analyze the applicability of other similar schemes in the given context and evaluate the time efficiency of both Shamir's secret-sharing scheme (Shamir, 1979) and the information dispersal algorithm presented by Rabin (1989), which is known for its space efficiency but "only" offers computational secrecy.

The current work is part of the ongoing TRESOR (TRusted Ecosystem for Standardized and Open cloud-based Resources) project (TRESOR, 2015) and is conducted in accordance with the design science frameworks proposed by Hevner et al. (2004) and in particular Peffers et al. (2008). Following the literature review framework proposed by vom Brocke (2009), we first started with a systematic literature review, where we observed the current research proposals on security and privacy protection for adoption of cloud computing in healthcare. Additionally, we conducted semi-structured interviews with different experts from the German healthcare industry, from which we derived real-world processes and corresponding security and privacy requirements. Based on these results, we designed our multi-provider cloud architecture that satisfies many of the requirements. Finally, we evaluated and selected a secret-sharing algorithm for our architecture, where we implemented both Shamir's secret-sharing scheme and Rabin's information dispersal algorithm and conducted several performance experiments.

The paper is structured as follows. The background on data protection in the context of cloud computing in healthcare is provided in Section 6.2. In Section 6.3, we present two use case scenarios where healthcare data is shared between two health centers, involving the processes of getting an appointment with a health center and medical admission in a health center. Sections 6.2 and 6.3 serve to illustrate the importance of the problem being addressed in this paper. Section 6.4 specifies the goals of our solution, describes the architecture design and demonstrates its functionality in three different scenarios. An overview and evaluation of Shamir's secret-sharing scheme and Rabin's information dispersal algorithm are given in Section 6.5. Finally, we discuss open challenges and make recommendations concerning future work in Section 6.6 before we conclude the paper.

6.2 Related Work

6.2.1 Literature Search

Following the approach proposed by vom Brocke et al. (2009), we searched across the EBSCOhost, IEEE Xplore, Emerald, ScienceDirect, AISeL, Springer, ACM Digital Library and Proquest databases. The keyword search in the domain of cloud computing in healthcare re-

sulted in 4222 publications, where we retrieved a final total of 11 dealing with security and privacy issues by screening titles and abstracts and five additional ones through a combined backward and forward search (see Table 19).

Database	EBSCOhost	IEEE Xplore	Emerald	ScienceDirect	AISeL	Springer	ACM Digital Library	Proquest	Sum Hits
Hits	2112	828	5	278	42	185	71	701	4222
Net Hits	2	4	0	1	0	3	1	0	11

Table 19. Results of the Keyword Search

6.2.2 Literature Analysis

Security and privacy threats for cloud-based medical data exchange scenarios are presented by Nematzadeh and Camp (2010), Shini et al. (2012), and Loehr et al. (2010). Security and privacy requirements with respect to medical data sharing in the cloud are investigated by Zhang and Liu (2010), Deng et al. (2011), and Deng et al. (2012).

The currently introduced security and privacy-enhancing mechanisms for the use of cloud computing in healthcare are aimed to improve access control (Asmuth and Bloom, 1983; Bessani et al., 2011; Chen et al., 2012a, 2012b; Li et al., 2010, 2012; Yu et al., 2010), keyword search over encrypted records (Li et al., 2011b), unlinkability between the patient and the electronic health record (Li et al., 2011a), traitor tracing (Nematzadeh and Camp, 2010), and secure data storage (Bessani et al., 2011).

Some of our ideas are similar to Bessani et al. (2011). However, we additionally address encryption of records and more sophisticated privacy issues, such as unlinkability between the medical records and patients, confidentiality of the existence of a medical record for a given patient, and confidentiality of patient identifiers (see Section 6.4.1). We also aim to achieve similar functionality proposed in the above-mentioned publications in our architecture as future work.

To our knowledge, none of the papers focuses to the same extent on the issue of “curious” cloud providers who could get access to sensitive data at a point in the future, if the decryption keys for the documents stored in the cloud are compromised, or if the encryption algorithm is broken or suffers from an insecure implementation.

6.3 Case Study

Based on semi-structured interviews with different experts from the German healthcare industry, in particular the heads of IT departments, project managers and medical staff of different hospitals, where the healthcare providers’ processes and problem areas were in the spotlight of discussion, we report on two examples for use cases where healthcare data is shared be-

tween at least two health centers. Moreover, we present some assumptions derived from the above-mentioned interviews.

In the first use case, a patient visits a cardiologist for testing who suggests the patient has to get surgery. The cardiologist turns to a health center and sends some record. The surgeon in the health center inspects the film and makes the decision whether the patient needs an immediate appointment, on how to schedule him, whether he still needs additional inspections, etc. A generalized process of getting an appointment with a health center is shown in Figure 5.

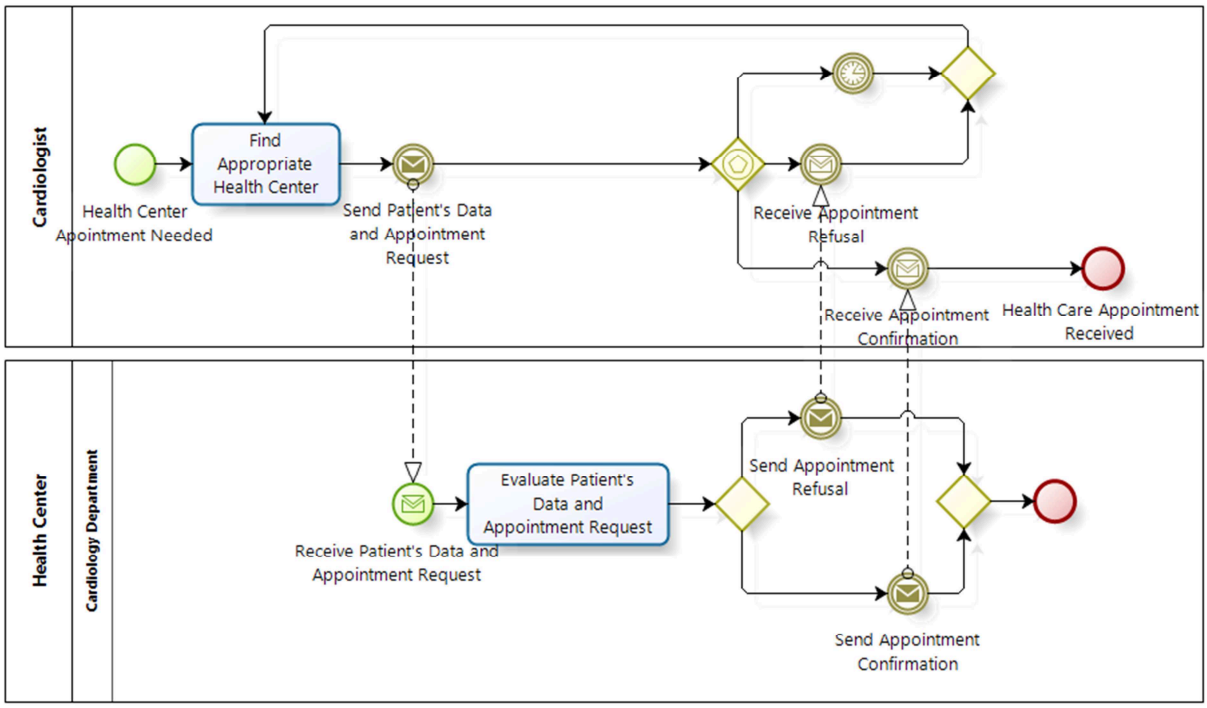

Figure 5. Generalized Process of Getting an Appointment with a Health Center

In the second use case, the doctor at the cardiology department needs to see the history of the patient before preparing a treatment plan. If other hospital stays of the patient are known, the information is requested from the previous hospital and often received in the form of a discharge letter. The medical report is a summary of the documents generated during the hospital stay and usually contains information on what has been done and what the recommended further therapy is (e.g., medication, check-up in 6 months). A generalized process of medical admission in a health center is presented in Figure 6. We use BPMN (Business Process Model and Notation) (OMG, 2014) to illustrate the processes of the first and second use cases in Figure 5and Figure 6, respectively.

From our case studies, also different scenarios for identifying EHR documents do emerge, which are relevant for our later discussion on the obfuscating document names:

Scenario 1: In the basic scenario, each EHR document for a patient can be assigned a unique *document ID* (D-ID), and these D-IDs are communicated to the next hospital by a physical document that comes with the patient. Each D-ID can be used as search key for relevant EHR documents in the clouds.

Scenario 2: In this scenario, we can assume that a patient has a unique and persistent *patient ID* (P-ID) across all hospital information systems, which he gets from a national registry or

during his first stay in a hospital. This P-ID, however, can be considered sensitive data when used in combination with health data, or even on its own if connected to location data. Therefore, its use in communication to external parties such as CPs should be obfuscated. In addition, each HC is using a unique HC-ID.

Scenario 3: In addition to the P-ID of scenario 2, we are provided with identifiers for each visit or case inside a HC. For each stay, there is a *case number* (Case-ID) assigned to the P-ID. All the documents created during the stay get an identifier assigned to the case number. However, those Case-IDs tend to be local to each HC, and are not known elsewhere. Here, a search strategy needs first to identify all Case-IDs for a patient at a certain HC, before the actual document retrieval can take place.

We refer to all those identifiers (D-ID, P-ID, HC-ID, Case-ID) as "internal identifiers", which should be obscured in communication to external parties, such as cloud providers by transforming them into "external identifiers". Our architecture will provide support for all three cases.

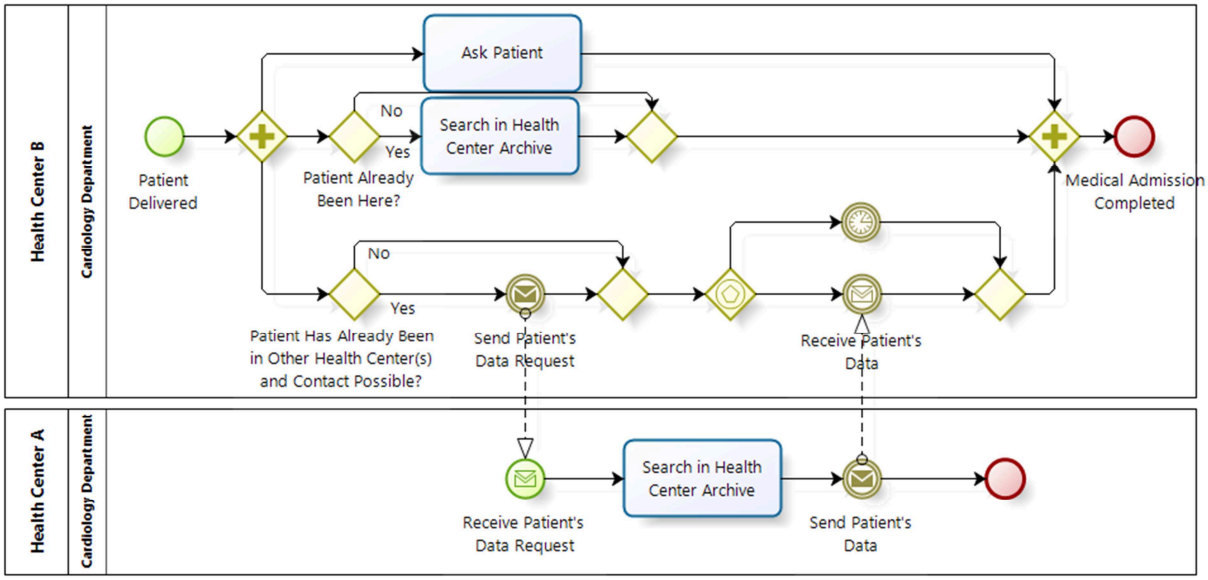

Figure 6. Generalized Process of Medical Admission in a Health Center

6.4 Architecture

6.4.1 Goals with Respect to Security and Privacy

Our aim is to satisfy the following main security and privacy goals with our architecture, which are derived from our case study and also confirmed as important by (Zhang and Liu, 2010; Basu et al., 2012; Chen et al., 2011, 2012a, 2012b; Deng et al., 2011; Li et al., 2010, 2011a, 2011b, 2012; Shini et al., 2012; Yu et al., 2010):

- Access control for preserving confidentiality and integrity of EHR content, internally and for inter-organizational partners.
- Confidentiality and integrity of the content of EHRs against external parties, including cloud providers.

- Confidentiality of the existence of an EHR for a given patient.
- Unlinkability between EHRs and patients.
- Confidentiality of patient identifiers, and their unlinkability with locations or health data. In particular, we should also enhance the confidentiality of the patient with respect to the potential profiling of his visits to HCs. In order to achieve this, the use of P-ID and other "internal identifiers" in communication to external parties such as CPs should be minimized, e.g., by transforming them into "external identifiers".
- Authenticity of EHRs during storage and transmission.
- Availability and authorized archiving of EHRs (by CPs).
- Efficiency, scalability, and usability.

In addition to this more data-centric view, classical security network measures described in Section 6.4.2 should protect all communications.

6.4.2 Security Measures

In order to satisfy the presented security and privacy requirements, our architecture features a combination of established and new building blocks (see Table 20). Currently, we assume that "data owners" are the health centers. We leave an extension of this assumption to multilateral security requirements (Fabian et al., 2010) and in particular the challenges of patient-centric data management for future work.

In our approach, we assume that all participating organizations, such as HCs or CPs, have a common interest in securing the infrastructure and data against external, third-party adversaries. Hence, the establishment of common and cooperative security mechanisms will be feasible, even though many practical and procedural challenges could arise when implementing them in concrete usage scenarios. We acknowledge these important challenges, but consider them out-of scope of our current paper.

In particular, we assume a cooperative infrastructure for Client and Service Authentication. This could involve a central Certificate Authority (CA), a tree or "forest" of CAs forming a Public-Key Infrastructure (PKI) or a fully connected Web-of-Trust between all participating organizations (Stallings, 2010). Any client program or service can be authenticated, preventing unauthorized third parties from taking part in the system simply by adopting a false identity.

Second, it is necessary that classical network security protocols be in place, which prevent eavesdropping or forging of any communication by third-party adversaries. Depending on the concrete realization of communication between partners, such protocols could include Virtual Private Networks (VPNs) between all cooperating partners, Transport Layer Security including HTTPS for Web-based information exchange (Stallings, 2010) or, more advanced, Web Service Security protocols, if a cooperative service-oriented architecture (SOA) is used (OASIS, 2014).

As an optional but recommended building block, Federated Identity Management and User Authentication could increase the usability of the system by providing a common view on user identities across organizational borders (Shim et al., 2005). Health centers cooperate by implementing local user identification and sharing authentication status-information according to a mutual trust relationship. Moreover, authenticated users at HCs can be authorized to

access documents stored at the CPs, which can be implemented by including the CPs as "consumers" of the federated identity management and authentication process.

Security Measure	**Goal**	**Locations**
Client and Service Authentication	Prevent unauthorized participation in the system	All participants
Network Security	Prevent communication eavesdropping or modification by unauthorized third parties	All participants
Federated Identity Management	Increase usability and reduce management overhead	Data owners (HCs), may be extended to CPs
Access Control (RBAC, TBAC), Attribute-Based Encryption of Documents	Fine-grained: protect access to sensitive information inside documents; coarse-grained: prevent unauthorized retrieval of documents from the clouds	Fine-grained at Data owners (HCs); coarse-grained document access control at CPs
Digital Signatures	Prevent unauthorized modification of documents	Data owners (HCs)
Internal Replication	Prevent data loss	CPs
Secret-Sharing	Increase availability of data by spreading it redundantly across multiple CPs; Prevent curious CPs from spying on data in case of key compromise	Data owners (HCs)
Cryptographic Hash Function for constructing "external identifiers"	Obfuscate the relation between documents and patient IDs or other "internal identifiers"	Data owners (HCs)

Table 20. Security Mechanisms

Authentication and (possibly federated) identities would serve as prerequisite for authorization. Here we propose that a framework of access-control policies authorizes participating HCs and their employees, and possibly also authorized external information clients. This would include Role-Based Access Control (RBAC), if there are clear correspondences between job roles and information demands (Ferraiolo et al., 2007) in a HC, or Task-Based Authorization Controls (TBAC), if access to information should be more ad hoc, dynamically depending on a specific task at hand (Thomas and Sandhu, 1997). Similar challenges of coordinated access control have been addressed for industry applications by (Kunz et al., 2010).

Depending on the granularity of access control, such policies could be technically enforced by access control mechanisms at HCs and CPs, but also by implementing advanced encryption methods that are operating on the documents stored in the clouds. We recommend a combination of both approaches: first, accessing any document in a participating cloud should be possible only for authorized clients. If additional advanced encryption methods are applied, this first line of access control could be coarse-grained, reducing the overhead (and possible information leakage) of communicating fine-grained policies to the CPs.

For example, in order to retrieve an encrypted document, a client may only need to provide proof that she is a member of an authorized HC. Fine-grained access control by encryption could enforce that only truly authorized individuals could decrypt sensitive information included in this document. Recent advances in this direction include Attribute-Based Document

Encryption, which allows fine-grained access control (Li et al., 2010, 2012) by encryption at the level of data attributes.

In order to provide protection against unauthorized modification of documents, we recommend the use of digital signatures issued by each organization at least at the document level before documents are stored in the clouds. We leave the possibility of signatures at an attribute-level or by individual persons for future work. Not least, every CP should provide internal redundancy and backup mechanisms against loss of documents, in order to achieve long-term availability of information. In addition, each HC needs to adopt procedures for storing and conserving cryptographic parameters and keys.

As a new contribution, we recommend the use secret-sharing schemes in order to even further reduce the risk of information leakage in multi-clouds, in particular to reduce the risks of encryption errors or compromise decryption keys in the face of curious cloud providers. Details of this procedure will be discussed in the next sections.

6.4.3 Multi-Cloud Secret-Sharing Architecture

The data owner, here a HC A, defines a policy for document storage and retrieval, which then is communicated to the CPs (Figure 7). The electronic health record (EHR) at A is assembled as a document D, and an access-control policy according to RBAC or TBAC models is designed. D is encrypted to E(D) according to the policy (by methods such as Attribute-Based Encryption), and digitally signed. The signature is attached to E(D). Now, according to a secret-sharing scheme, E(D) is split into several shares (see Section 6.5 for details).

For each share, a pseudonymous external identifier is constructed from available internal identifiers, depending on the scenario (see Section 6.3). These external identifiers serve as search keys for the document shares (which look like random bit strings) at each cloud provider.

Scenario 1: The external identifier is calculated by applying the cryptographic hash function SHA-1 (Eastlake and Jones, 2001; Stallings, 2010) to the concatenation of the document identifier D-ID and an integer-valued Share-ID identifying the share: External-ID := sha-1(D-ID, Share-ID). This results in a pseudorandom string of 160 bits.

Scenario 2: Using the unique internal patient identifier P-ID and its own HC identifier HC-ID as inputs, the software at the HC calculates the cryptographic hash of concatenated identifiers: sha-1(P-ID, HC-ID, Share-ID). This hash value does not provide any sensitive information about the patient identity to an external party or a CP, since it is nearly impossible to invert the hash function. We leave countermeasures against dictionary attacks to future work.

Scenario 3: This scenario is more complex, since case identifiers are known only to the issuing HC. Here, another document L is needed that collects all Case-IDs per patient and HC. Such a document would be small, and could be split across all CPs in a similar way as the main data documents. We leave out the technical details, only state that when a new case is opened, first L is retrieved (identified by sha-1(P-ID, HC-ID, Share-ID) as in Scenario 2) and the current Case-ID is added. All shares of the actual case-based EHR documents are identified by sha-1(P-ID, HC-ID, Case-ID, Share-ID) during storage and retrieval. Again, no sensitive internal identifier is leaked to external parties such as CPs.

Once external identifiers are established, each share is stored at a different cloud provider using the external identifier for future retrieval (Figure 8). Every cloud provider then takes care of data replication inside his own cloud. This process can be executed at each HC.

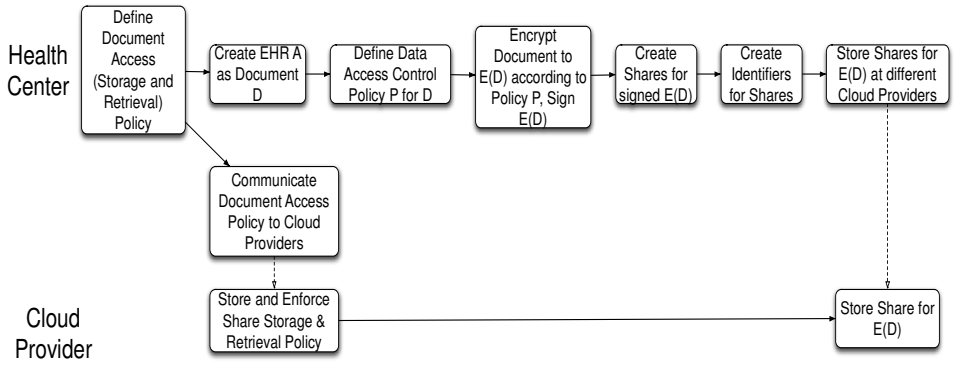

Figure 7. Storage Process

In all scenarios, external identifiers are constructed in such a way that later on authorized clients can calculate identifiers and retrieve the data using an analogous procedure.

The retrieval process is similar to the storage process (Figure 8). If a patient arrives at a new HC C, the patient history needs to be retrieved, i.e., all EHRs for the patient should be retrieved from the clouds. External identifiers for document shares are constructed in the same way as in the storage process, depending on the scenario.

For each document, at least threshold t (see Section 6.5.1) many shares are retrieved (this involves authentication to the CPs) and recombined into E(D). The attached signature is verified. The still encrypted documents can be handed over to a client program of the information requester, which can decrypt parts of the documents according to the requester's authorization and decryption keys.

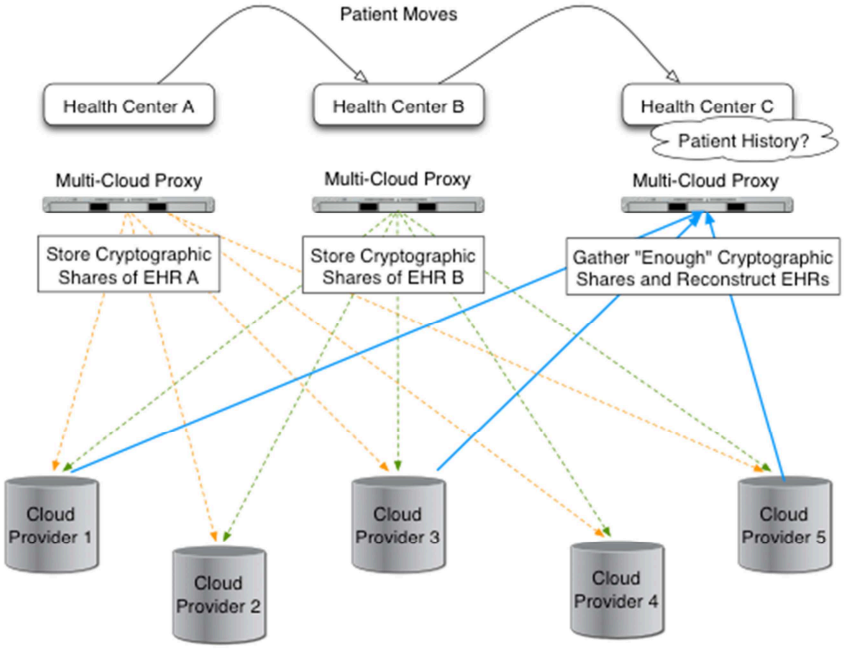

Figure 8. Conceptual Architecture for Secret Sharing in Multi-Provider Clouds

6.5 Evaluation of Secret Sharing Methods

6.5.1 Introduction to Secret-Sharing Schemes

A secret-sharing scheme is often defined as a "threshold scheme". We follow the definition of secret-sharing schemes given by Stinson (1992). Let t, n be positive integers. Then a (t, n)-threshold scheme is a method of sharing a secret among a finite set of participants R in such a way that any t (or more) participants can compute the value of the secret, but no group of t-1 (or fewer) participants can do so. While distributing the secret among participants in R, each participant is given some partial information called a share. The shares are distributed secretly, so that no participant knows the share given to another participant. If n is larger than t, such a scheme can provide data redundancy for increased availability, since some shares can get lost without preventing the reconstruction of the secret by authorized entities.

Secret-sharing methods were introduced independently by Shamir and Blakley in 1979. Blakley's solution uses finite geometries, while Shamir's scheme (SSSS) is based on polynomial interpolation. The information dispersal algorithm (IDA) proposed by Rabin (1989) may also be considered a secret-sharing scheme for computationally bounded adversaries. In contrast to SSSS, IDA's (t, n)-threshold scheme describes the secret by the whole polynomial. A fundamentally different approach of secret sharing is the scheme proposed by Asmuth and Bloom (1983). Here, the shares are obtained by using modular arithmetic and the secret is reconstructed by the application of Chinese Reminder Theorem.

Shamir's secret-sharing scheme (Shamir, 1979) and Rabin's information dispersal algorithm (Rabin, 1989) are known for perfect privacy and space efficiency, respectively. Shamir's secret-sharing scheme makes the document absolutely undetermined when there are t-1 or fewer shares available. Rabin's information dispersal algorithm produces pieces of a length t-times less than the original document. Furthermore, those algorithms are the most often discussed in the literature and have been adopted in multiple applications, such as Rodrigues and Liskov (2005), Fabian et al. (2012), Geambasu et al. (2009), and Mills and Znati (2008).

Krawczyk (1994) introduced a combination of Shamir's secret-sharing scheme, encryption, and Rabin's information dispersal algorithm. The scheme proves to be space and communication efficient and secure given a secure encryption function. Distributed fingerprints provide the scheme with robustness, namely, the ability to recover the secret in the presence of a bounded number of corrupted shares (Krawczyk, 1993).

The main principles of Shamir's secret-sharing scheme (Shamir, 1979) and Rabin's information dispersal algorithm (Rabin, 1989) can be described as follows. Given a secret s (i.e., the document itself or a data block of it) and parameters t and n, Shamir's scheme sets $a_0 = s$, randomly chooses $a_1,...,a_{t-1}$ and distinct $x_1,...,x_n$, and calculates the shares as:

$$(x_i, y_i = f(x_i) = \sum_{j=0}^{t-1} a_j x_i^j), i \in \{1, n\}. \qquad (1)$$

For reconstructing the secret, the Lagrange interpolating polynomial is calculated at x=0 using the formula:

$$L(x) = \sum_{j=1}^{t} y_j \prod_{k=1, k \neq j}^{t} \frac{x - x_k}{x_j - x_k}. \quad (2)$$

Under the same assumptions, IDA splits the secret of length N into blocks of length t:

$$s = (a_1,...,a_t)(a_{t+1},...,a_{2t}),...,(a_{N-t+1},...,a_N). \quad (3)$$

The algorithm randomly chooses distinct $x_1,...,x_n$ and calculates the shares as $(x_i, y_i = (y_{i1},..., y_{i(N/t)})), i \in \{1, n\}$ from:

$$\begin{bmatrix} x_1^0 & \dots & x_1^{t-1} \\ \dots & \dots & \dots \\ x_n^0 & \dots & x_n^{t-1} \end{bmatrix} \begin{bmatrix} a_1 & \dots & a_{N-t+1} \\ \dots & \dots & \dots \\ a_t & \dots & a_N \end{bmatrix} = \begin{bmatrix} y_{11} & \dots & y_{1(N/t)} \\ \dots & \dots & \dots \\ y_{n1} & \dots & y_{n(N/t)} \end{bmatrix}.$$

Given the shares, the secret can be easily reconstructed by solving the system of linear equations.

In order to evaluate and select a secret-sharing algorithm for our multi-cloud architecture, we implemented both Shamir's secret-sharing scheme and Rabin's information dispersal algorithm. With Shamir's scheme, we also improved an established share reconstruction method by a newly designed approach based on Lagrange interpolation.

We performed several experiments on consumer-grade hardware, a notebook with Mac OS X (Intel Core 2 Duo, 2.4 GHz, 4 GB RAM), and measured the execution time (in milliseconds) required for splitting and recovering documents of different sizes: from 32 bytes, representing for example the short list L of Scenario 3 in Section 6.3, to 1 megabyte with different thresholds (from 4 to 9).

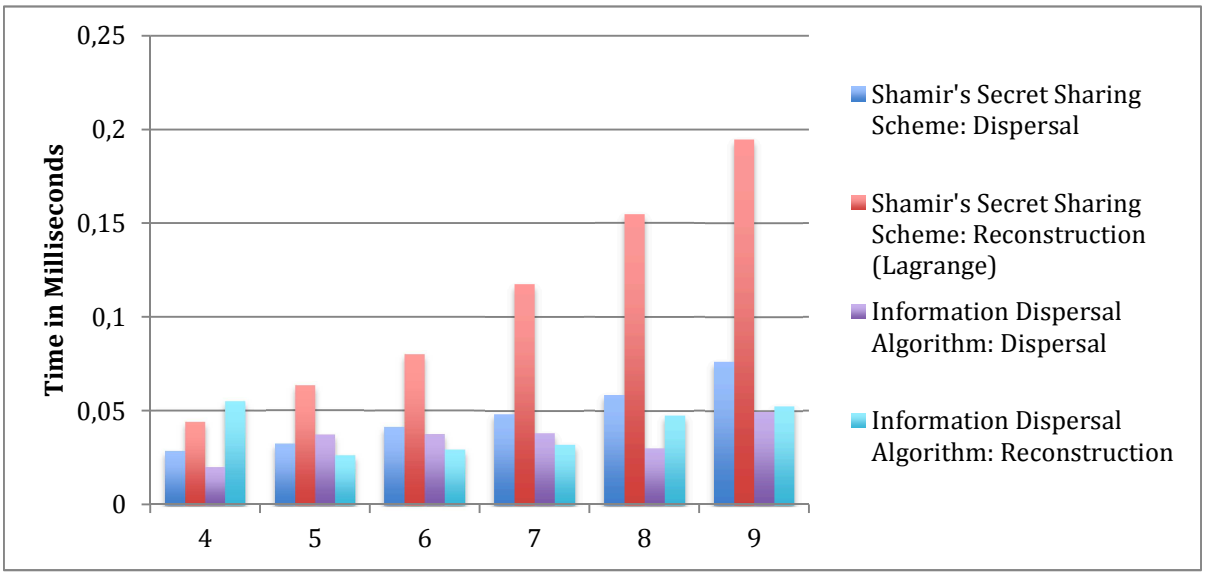

Figure 9. Comparison of Shamir's and Rabin's Algorithms for 32 Byte Documents for Varying Thresholds t

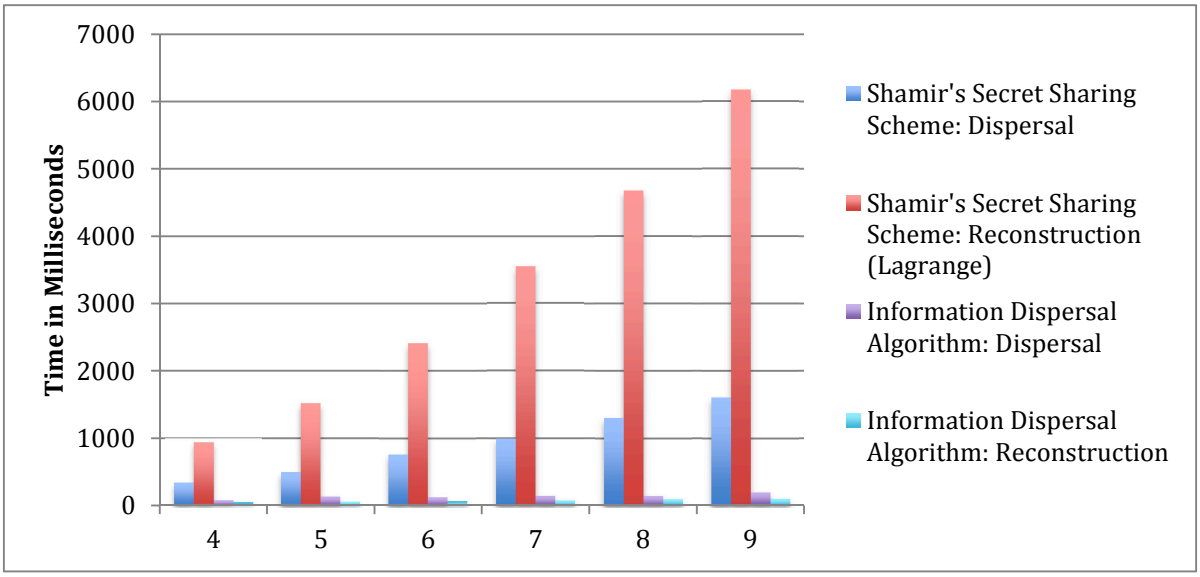

Figure 10. Comparison of Shamir's and Rabin's Algorithms for 1 MB Documents for Varying Thresholds t

For simplicity, we generated exactly as many shares in each case as necessary for further reconstruction, i.e., t=n. Each experiment was repeated 10,000 times, and the average was calculated in order to eliminate the influence of possible random outliers.

As our experimental results in Figure 9 and Figure 10 show, Shamir's secret-sharing scheme works slower than Rabin's information dispersal algorithm. Furthermore, especially the Shamir reconstruction process has a huge marginal increase when the document size or the threshold grows, despite our optimization by Lagrange interpolation.

6.5.2 Discussion and Recommendations

Our experimental results give good indicators to the low computational overhead of adding our secret-sharing approach to a multi-cloud environment, even on consumer grade hardware. This will be important for integrating patients as active participants into our architecture. In particular, we recommend and aim to adopt Rabin's information dispersal algorithm in our setting. Concerning potential communication overhead, we will design corresponding experiments once the implementation of the proxy and other components of our infrastructure have matured. But since Rabin's approach produces much smaller shares, we also expect it to perform superior in this aspect.

6.6 Open Challenges and Future Work

Our main goal for future work is the full implementation of the cloud secret-sharing proxies, and their test in real networks using different real-world clouds. On the organizational side, corresponding security assumptions and processes will be evaluated with practice partners in healthcare, including signatures at an attribute-level or by individuals. In the future, we also aim to better involve the patient into our architecture. This could involve the inclusion of the patient as an actor, e.g., giving him or her control over shares of their EHRs. Moreover, we aim to address some of the corresponding research challenges seen as open by Loehr et al.

(2010) and Zhang and Liu (2010). In particular, the problem of ownership of information, the feasibility of reliable auditing, patient consent for data access and access revocation can involve interesting challenges for our research and practice.

6.7 Conclusion

Starting from real-world case studies, this paper provided example processes for inter-organizational health data sharing, and motivated the usefulness of such a cloud environment. We indicated corresponding security and privacy challenges, and presented our multi-provider cloud architecture. In addition to classical encryption and other security measures, this architecture features secret-sharing as an important measure to distribute EHRs as fragments to different cloud providers, providing an additional privacy protection in the case of key compromise, or if encryption algorithms are broken or their implementation turn out to be insecure.

In order to evaluate and select a secret-sharing algorithm for our multi-cloud architecture, we implemented both Shamir's secret-sharing scheme and Rabin's information dispersal algorithm and performed experiments on splitting and recovering documents. These experiments indicate a low computational overhead, giving good indicators to the feasibility of our architecture, which we aim to develop further towards a full implementation in the future.

7. Evaluation of Improvement in Acceptance of Health Clouds

Title	Improving Acceptance of Health Clouds
Authors	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
Published in	In Submission (Ermakova et al., 2015b)
Abstract	*Background*: Cloud computing promises essential improvements in medical service delivery processes. However, patients' worries about their medical data protection might be a source of adoption hurdles. *Objectives*: This study examines the effectiveness of confidentiality assurances with regard to the willingness of potential patients to provide consent to healthcare providers for sharing their medical records over a cloud. *Methods*: We base on a recently proposed multi-cloud architecture which features security through a secret-sharing mech-anism: Confidential health information is cryptographically encoded and distributed in a way that no single and no small group of cloud providers is able to decode it. We empirically evaluate this by a survey with over 260 full responses. *Results*: The results indicate that this confidentiality assurance makes individuals significantly more willing to accept health clouds for sensitive health information shared by healthcare professionals. Our study further shows that individuals are more likely to accept health clouds in emergency cases. When time conditions are not critical, patient consent is rather to be obtained for transmission of non-sensitive or pseudonymized medical records. In the presence of casual offline means, individuals' willingness to accept health clouds significantly falls when compared to other investigated cases. *Conclusions*: In general, this study demonstrates that individuals' acceptance of health clouds could be strengthened with stronger confidentiality assurances with respect to their medical records to be shared for health provision, in particular through secret sharing. With this approach, health clouds would become more popular even when there are casual offline options to deliver patient data. In addition to the mechanism, personal identifiers or sensitive details could be excluded.
Keywords	Cloud Computing, Healthcare, Acceptance

7.1 Introduction

Adopting cloud computing in the medical field can improve medical service delivery processes (Sultan, 2014a, 2014b; Haskew et al., 2015). In particular, cloud computing offers opportunities to resolve several collaborative issues among healthcare professionals and facilitates timely delivery of medical records wherever they are needed (Wu et al., 2012; Karthikeyan and Sukanesh, 2012; Poulymenopoulou et al., 2011; Rolim et al., 2010; Koufi et al., 2010; Ahuja et al., 2012; Haskew et al., 2015). Cloud computing implies a model where virtual machines, development tools and software are provided just on demand, usually over the Internet (e.g., Mell and Grance, 2012). According to the McKinsey Global Institute's estimates, cloud computing has the potential to affect $3 trillion in worldwide enterprise IT spending (Manyika et al., 2013). Nevertheless, recent research indicates that the control over the data stored and processed by cloud computing's third-party providers is commonly perceived as lost (Chow et al., 2009; Ion et al., 2011). In particular, patients' privacy fears with respect to their medical information could be an essential obstacle for healthcare professionals to adopt health clouds in their medical service delivery practice (Ermakova et al., 2014a).

Prior work suggests that individuals' privacy concerns get weaker the higher people regard technological mechanisms as being capable of preserving their privacy (Dinev et al., 2012; Ermakova et al., 2014a). In the light of this finding, the present study validates and more tightly examines the efficacy of higher confidentiality assurances as a means of increasing acceptance of health clouds among individuals. In particular, it explores individuals' willingness to provide consent for sharing their medical records over the cloud. This work further extends previous research by separately considering a variety of circumstances. For determining and measuring the above mentioned effect, the study bases on the recently introduced multi-provider cloud architecture that provides confidentiality of the stored or transmitted medical records even in the cases of compromised encryption keys and broken or insecurely implemented encryption algorithms (Ermakova and Fabian, 2013; Fabian et al., 2014). Encrypted health records are proposed to be divided into different fragments by a secret-sharing scheme (Shamir, 1979). The fragments are then to be distributed among several independent cloud services. The mechanism guarantees the reconstruction of the initial document in the presence of a given number of document shares; otherwise, the reconstruction is absolutely impossible.

Furthermore, previous empirical studies report on lower privacy concerns (Nass et al., 2009) and stronger acceptance of health information sharing in the absence of personal identifiers (Whiddett et al., 2006; Perera et al., 2011; Riordan et al., 2015). The type of shared health information was found essential in formation of individuals' attitudes (Zulman et al., 2011), whereas its sensitivity was shown to impact privacy concerns (Bansal et al., 2007, 2010). Referring to this evidence, we further elaborate on the importance of some background in establishment of individuals' acceptance of health clouds.

To summarize, the present study attempts to answer following research questions: (1) Can higher confidentiality guarantee an increase in individuals' acceptance of health clouds? (2) Does individuals' acceptance of health clouds depend on a situational context?

This work is organized as follows: Section 7.2 starts with providing some background on acceptance of health clouds and related health information privacy concerns and health information sensitivity. In the following section, we describe the methodology we used. We then present the study results in Section 7.4 and discuss the findings in Section 7.5. Finally, we

summarize them and derive suggestions for future research and implications for theory and practice.

7.2 Background and Related Work

A timely delivery of medical records where they are needed is essential for medical service delivery and can be facilitated through cloud computing capabilities (Wu et al., 2012; Karthikeyan and Sukanesh, 2012; Poulymenopoulou et al., 2011; Rolim et al., 2010; Koufi et al., 2010; Ahuja et al., 2012; Haskew et al., 2015). Although individuals generally speak in support of electronic exchange of health information among healthcare providers (Perera et al., 2011; Ancker et al., 2012a, 2012b; Simon et al., 2009), patient consent to share medical records this way is not easily obtained (Ermakova et al., 2014a; Riordan et al., 2015). Individuals are afraid of potential risks to their health information travelling over the Internet (Perera et al., 2011; Ancker et al., 2012a, 2012b; Simon et al., 2009). As a result of medical records' misuse, patients might become subject to harassment by healthcare product marketers, discrimination by employers, healthcare insurance agencies and associates, and other harms (Bansal et al., 2010; Laric et al., 2009; Rohm and Milne, 2004; Cushman et al., 2010; Duquenoy et al., 2012; Appari and Johnson, 2010). Recent empirical evidence demonstrates that consent decreases the more individuals are concerned about what can happen to the data (Ermakova et al., 2014a).

As argued by McGraw et al. (2009), revealing de-identified health information to third parties for purposes of research and business intelligence complies with Health Insurance Portability and Accountability Act (HIPAA) (U.S. Department of Health and Human Services, 2015). Studies show that individuals are then less worried (Nass et al., 2009) and more willing to accept health information sharing without personal identifiers (Whiddett et al., 2006; Perera et al., 2011; Riordan et al., 2015). Nonetheless, removing direct identifiers from medical records does not guarantee that health information is fully protected in terms of privacy (King et al., 2012; McGraw et al., 2009; Li et al., 2011).

Individuals' attitudes toward sharing their health information are further influenced by the type of information being shared (Zulman et al., 2011). Perceived health information sensitivity impacts concern formation (Bansal et al., 2007, 2010). Unhealthy individuals are more vulnerable to negative consequences as a result of their medical records' misuse and are thus more concerned about their privacy (Laric et al., 2009).

This study relies on a novel multi-provider cloud architecture (Ermakova and Fabian, 2013; Fabian et al., 2014). In comparison to other mechanisms proposed to preserve privacy in health clouds (Abbas and Khan, 2014), it guarantees confidentiality of medical records even when encryption keys will be compromised or encryption algorithms will be broken or insecurely implemented. In this architecture, encrypted health records are divided into different fragments by a secret-sharing scheme (e.g., Shamir, 1979; Rabin, 1989; Krawczyk, 1994). The document shares are distributed among different cloud services. The secret-sharing mechanism guarantees that a reconstruction of the initial document is only possible in the presence of a certain number of document shares. Therefore, single or small groups of malicious cloud providers are not able to break the confidentiality of health records. In this study, we particularly rely on a perfect secret-sharing scheme (e.g., Shamir's secret-sharing scheme) as a main feature of the multi-provider cloud architecture. Given less document shares than necessary for the document recovery, perfect secrecy ensures absolutely no information leakage (Krawczyk, 1994).

7.3 Methods

7.3.1 Sample

We invited people in Germany and Switzerland to participate in our online study via mailing lists as well as personally and collected responses from November 2013 until January 2014. All participants were informed about our study objectives and were encouraged to learn about cloud computing before taking part in the survey.

7.3.2 Data Collection

To conduct this study, we developed a questionnaire which contained 14 questions. Specifically, the subjects were presented the health cloud application scenario and asked to indicate their intention to permit medical workers to transfer their encrypted sensitive patient data over clouds for seven hypothetical cases (Table 21). Then, we shortly gave an idea of how this would work in the multi-cloud setting and asked the same questions as before (Table 22). The participants were not presented any other specific information to avoid potential confounding effects. Each question could be answered using a 7-point Likert scale – 1: Not likely at all, 2: Highly unlikely, 3: Rather unlikely, 4: Neither likely nor unlikely, 5: Rather likely, 6: Highly likely, 7: Fully likely. Before starting, we validated the survey with multiple individuals of different age, gender and education.

7.3.3 Analysis

We analysed the collected data in the R 3.8 computing environment (R Development Core Team, 2012). We applied the paired Student's t-test (e.g., Sheskin, 2004, pp. 580-585; Lowry, 2013) and the paired Wilcoxon signed-rank test (Lowry, 2013). The paired tests are appropriate to compare repeated measurements on the same sample. Student's t-test was similarly used by Perera et al. (2011), Teixeira et al. (2011), and Acquisti and Gross (2006), Wilcoxon signed-rank test was applied by Acquisti and Gross (2006). The t statistic measures a ratio between the tested effect size and the standard error of that effect. A larger ratio means that the effect size is stronger and allows to conclude that the effect size is not due to a chance (Li and Baron, 2012, p. 100). Although Student's t-test requires the population to be normally distributed, due to the Central Limit Theorem, the requirement can be regarded as approximately fulfilled for larger samples ($n >= 30$), as in our case. Wilcoxon signed-rank is based on summation of signed ranks (Lowry, 2013). It is commonly seen as an alternative to Student's t-test when normal distribution of the population cannot be assumed.

7.4 Results

7.4.1 Participants' Demographic Characteristics and Acceptance of Health Clouds

266 of the 464 surveys (57.33%) were fully completed. The participants have mean age of 27.93 years with a standard deviation of 9 years. A slight majority of them are female (53.01%). 5 (1.88%) and 2 (0.75%) did not state their gender and age, respectively.

	Not likely at all	Highly unlikely	Rather unlikely	Neither likely nor unlikely	Rather likely	Highly likely	Fully likely
	1	2	3	4	5	6	7
"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."	15	15	24	10	50	80	72
	5.64%	5.64%	9.02%	3.76%	18.80%	30.08%	27.07%
"… it is an emergency situation."	8	6	8	4	38	67	135
	3.01%	2.26%	3.01%	1.50%	14.29%	25.19%	50.75%
"… your patient data could otherwise be transferred via fax."	35	28	36	32	36	47	52
	13.16%	10.53%	13.53%	12.03%	13.53%	17.67%	19.55%
"… your patient data could otherwise be transferred via taxi."	34	22	28	24	37	50	71
	12.78%	8.27%	10.53%	9.02%	13.91%	18.80%	26.69%
"… you would have to deal with the transmission yourself."	36	29	35	18	47	42	59
	13.53%	10.90%	13.16%	6.77%	17.67%	15.79%	22.18%
"… the part of your patient data you consider to be sensitive is not transferred."	10	6	26	16	40	72	96
	3.76%	2.26%	9.77%	6.02%	15.04%	27.07%	36.09%
"… your patient data is pseudonymized (a pseudonym is used instead of your personal identifying data) before being encrypted."	13	12	17	22	52	55	95
	4.89%	4.51%	6.39%	8.27%	19.55%	20.68%	35.71%

Table 21. Distribution of Survey Participants' Acceptance of Health Clouds in the Absence of Additional Confidentiality through Secret Sharing

Table 21 and Table 22 provide overviews over responses regarding acceptance of health clouds. While all instruments asked the respondent to rank his or her behavioural intention to accept health clouds on a 7-point Likert scale, the questions were rather specific. The first group of questions paid attention to health clouds as facilitators of timely delivery of medical records (i.e., "*how likely would you approve to the transmission if*" ["*your patient data could otherwise arrive not in time*" | "*it is an emergency situation*"]?). Further questions focussed on health clouds as an alternative to casual offline transfer means for medical data (i.e., "*how likely would you approve to the transmission if*" ["*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 remaining items intended to explore health clouds with regard to less sensitive medical data (i.e., "*how likely would you approve to the transmission*" ["*if the part of your patient data you consider to be sensitive is not transferred*" | "*your patient data is pseudonymized (a pseudonym is used instead of your personal identifying data) before being encrypted*"]?).

	Not likely at all	Highly unlikely	Rather unlikely	Neither likely nor unlikely	Rather likely	Highly likely	Fully likely
	1	2	3	4	5	6	7
"Imagine that your sensitive patient data could be encrypted and sent in single fragments from your current medical institution to another (a hospital or a doctor) just in the right moment using different cloud-based systems, where it would be reassembled. *Only a relatively large amount of fragments can be used to reassemble your encrypted patient data, otherwise there is absolutely no leakage of information about it. Therefore, no single cloud provider or even small groups of cloud providers can access your encrypted data.* *Given the above mentioned circumstances, how likely would you approve to the transmission if …"*							
"… your patient data could otherwise arrive not in time."	10	9	14	10	47	84	92
	3.76%	3.38%	5.26%	3.76%	17.67%	31.58%	34.59%
"… it is an emergency situation."	7	5	5	5	33	51	160
	2.63%	1.88%	1.88%	1.88%	12.41%	19.17%	60.15%
"… your patient data could otherwise be transferred via fax."	22	22	23	20	48	61	70
	8.27%	8.27%	8.65%	7.52%	18.05%	22.93%	26.32%
"… your patient data could otherwise be transferred via taxi."	22	14	20	30	39	48	93
	8.27%	5.26%	7.52%	11.28%	14.66%	18.05%	34.96%
"… you would have to deal with the transmission yourself."	27	22	28	19	39	50	81
	10.15%	8.27%	10.53%	7.14%	14.66%	18.80%	30.45%
"… the part of your patient data you consider to be sensitive is not transferred."	13	11	15	17	41	60	109
	4.89%	4.14%	5.64%	6.39%	15.41%	22.56%	40.98%
"… your patient data is pseudonymized (a pseudonym is used instead of your personal identifying data) before being encrypted."	16	7	11	26	40	65	101
	6.02%	2.63%	4.14%	9.77%	15.04%	24.44%	37.97%

Table 22. Distribution of Survey Participants' Acceptance of Health Clouds with Additional Confidentiality through Secret Sharing

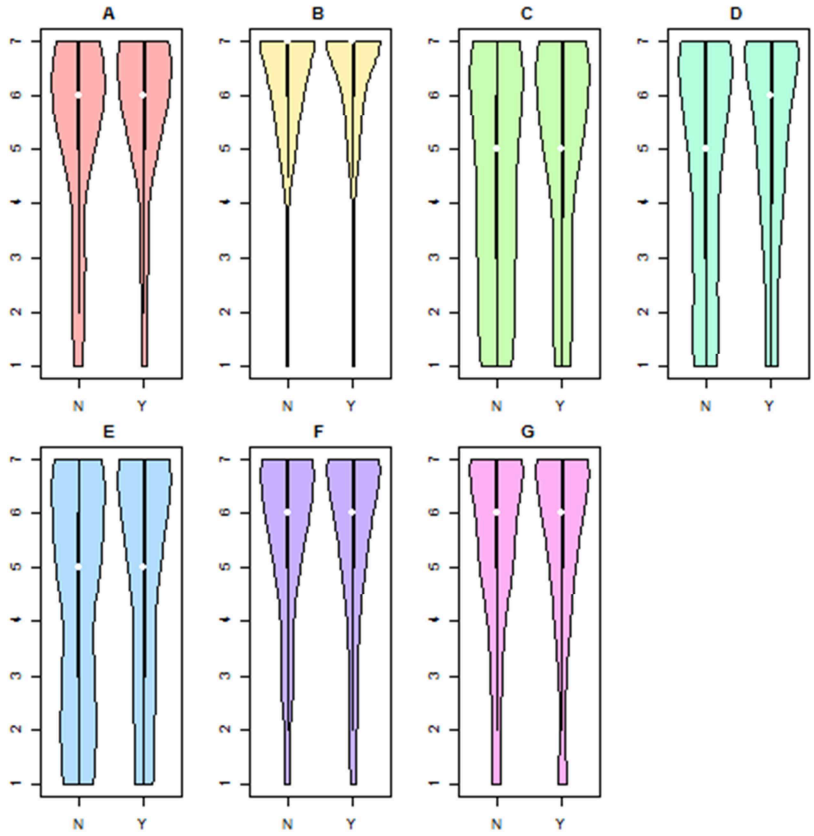

Figure 11. Violin Plots of Distribution of Behavioral Intention to Accept Health Clouds Without (N) vs. With (Y) Additional Confidentiality through Secret Sharing (see Table 23 for Abbreviations)

	1st Qu.	Median	Mean	3rd Qu.	Sd
Respondents' behavioral intention to accept the transfer of their encrypted sensitive patient data over cloud without (vs. with) additional confidentiality through secret sharing if …					
… this data could otherwise arrive not in time. (A)	5 (5)	6 (6)	5.24 (5.63)	7 (7)	1.78 (1.57)
… it is an emergency situation. (B)	6 (6)	7 (7)	6.01 (6.19)	7 (7)	1.44 (1.36)
… this data could otherwise be transferred via fax. (C)	3 (3.75)	5 (5)	4.33 (4.94)	6 (7)	2.06 (1.94)
… this data could otherwise be transferred via taxi. (D)	3 (4)	5 (6)	4.67 (5.14)	7 (7)	2.12 (1.94)
… this data has otherwise to be transferred by individuals. (E)	3 (3)	5 (5)	4.41 (4.87)	6 (7)	2.11 (2.07)
… the sensitive part of this data is not transferred. (F)	5 (5)	6 (6)	5.52 (5.56)	7 (7)	1.64 (1.73)
… the data is pseudonymized before encryption. (G)	5 (5)	6 (6)	5.39 (5.52)	7 (7)	1.73 (1.71)

Table 23. Summary Statistics for Respondents' Acceptance of Health Clouds

7.4.2 Does Additional Confidentiality through Secret Sharing Improve Individuals' Acceptance of Health Clouds?

As Table 23 demonstrates, survey respondents are on average more willing to accept health clouds in the presence of additional confidentiality assurances under every single circumstance (with a mean of 5.63 vs. 5.24 (A), 6.19 vs. 6.01 (B), 4.94 vs. 4.33 (C), 5.14 vs. 4.67 (D), 4.87 vs. 4.41 (E), 5.56 vs. 5.52 (F), and 5.52 vs. 5.39 (G)). Interestingly, their intentions are closer to the mean (with a standard deviation of 1.57 vs. 1.78 (A), 1.36 vs. 1.44 (B), 1.94 vs. 2.06 (C), 1.94 vs. 2.12 (D), 2.07 vs. 2.11 (E), 1.73 vs. 1.64 (F), and 1.71 vs. 1.73 (G)).

Figure 11 generally illustrates that there are more people supporting health clouds than those opposing them. This can also be observed in Figure 12 which shows scatterplots of the respondents' likeliness to approve the transmission of their encrypted sensitive patient data over a cloud-based system without (x-axis) versus with (y-axis) additional confidentiality through secret sharing with the trend line and identity line (dotted). The figure indicates that the trend lines are steeper sloped than the identity lines. It indicates that the participants tended to have higher likeliness to approve the transmission of their encrypted sensitive patient data over a cloud-based system when additional confidentiality through secret sharing was provided.

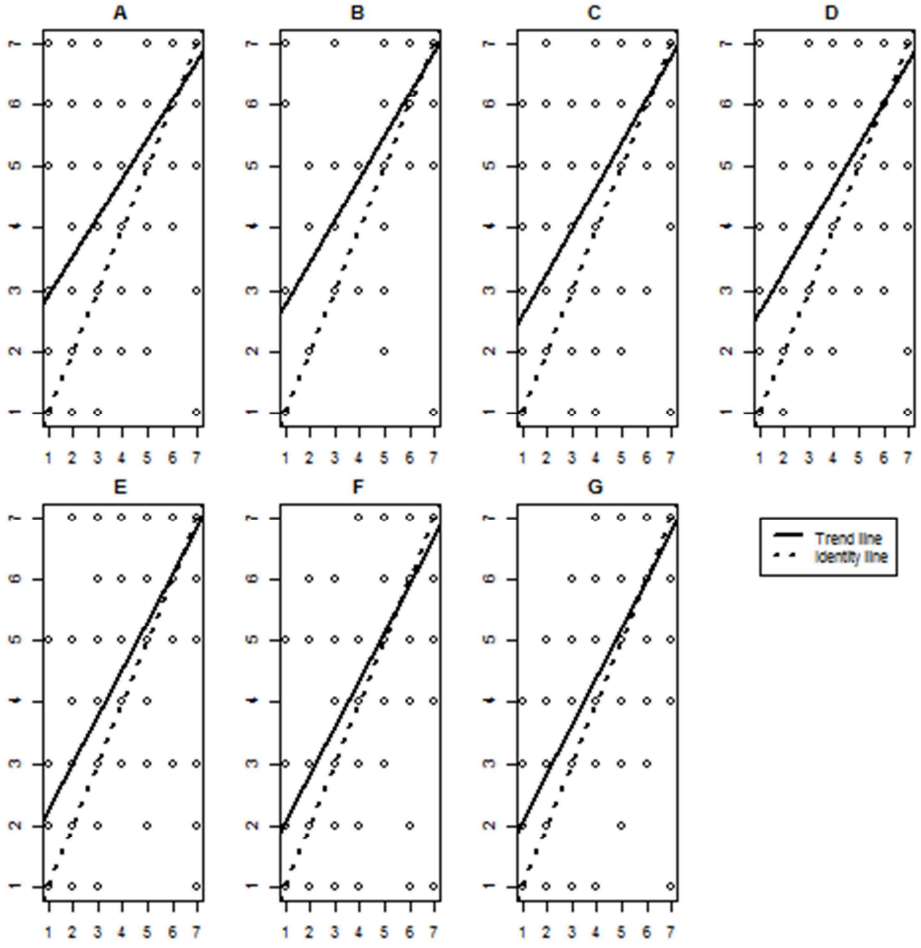

Figure 12. Scatterplots of Respondents' Likeliness to Accept the Transfer of Their Encrypted Sensitive Patient Data over Cloud Without (x-Axis) vs. With (y-Axis) Additional Confidentiality through Secret Sharing (see Table 23 for Abbreviations)

Hypothesis	Student's t-test	Wilcoxon signed rank test
Additional confidentiality through secret sharing increases individuals' likeliness to approve the transmission of their encrypted sensitive patient data over a cloud-based system, if …		
… this data could otherwise arrive not in time.	t = 4.86, p = 1.004e-06	V = 5360, p = 4.401e-07
… it is an emergency situation.	t = 2.75, p = 0.00317	V = 2978, p = 0.000262
… this data could otherwise be transferred via fax.	t = 6.88, p = 2.202e-11	V = 8330, p = 3.421e-11
… this data could otherwise be transferred via taxi.	t = 5.15, p = 2.606e-07	V = 6457.5, p = 8.592e-08
… this data has otherwise to be transferred by individuals themselves.	t = 5.36, p = 8.989e-08	V = 6143, p = 1.256e-08
… the sensitive part of this data is not transferred.	t = 0.54, p = 0.2933	V = 5321, p = 0.2494
… the data is pseudonymized before encryption.	t = 1.89, p = 0.03017	V = 4103.5, p = 0.01322

Table 24. Comparisons of Individuals' Acceptance of Health Clouds

Both Student's t-test and Wilcoxon signed rank test generally confirm that the positive effect of additional confidentiality promises is statistically significant (Table 24). Only in the least privacy-sensitive base case, i.e., where the sensitive part of patient data was not transmitted, the increase in individuals' acceptance of health clouds was found not to be significant (t = 0.5445, p-value = 0.2933; V = 5321, p-value = 0.2494). Regarding pseudonymized medical records, the raise in willingness could be confirmed only at a significance level of 5 % (t = 1.8864, p-value = 0.03017; V = 4103.5, p-value = 0.01322).

7.4.3 Does Individuals' Acceptance of Health Clouds Depend on a Situational Context?

As Table 23 demonstrates, health clouds are on average regarded as highly likely to be accepted in emergency cases (mean = 6.01 (6.19), standard deviation = 1.44 (1.36)). An average survey participant is more than rather willing to accept health clouds for timely delivery of his or her medical records (mean = 5.24 (5.63), standard deviation = 1.78 (1.57)). Health clouds are on average more than rather welcome for non-sensitive (mean = 5.52 (5.56), standard deviation = 1.64 (1.73)) and pseudonymized medical records (mean = 5.39 (5.52), standard deviation = 1.73 (1.71)). In the presence of casual offline options to health clouds, i.e., fax (mean = 4.33 (4.94), standard deviation = 2.06 (1.94)), self-service (mean = 4.41 (4.87), standard deviation = 2.11 (2.07)), and especially taxi (mean = 4.67 (5.14), standard deviation = 2.12 (1.94)), health clouds are generally viewed as somewhat less than rather favourable.

Both Student's t-test and Wilcoxon signed rank test confirm that many of mean differences are statistically significant (Table 25). We found evidence that higher levels in acceptance of health clouds are significant when one's medical condition becomes an emergency (B vs. A-G, with p-value < 2.2e-16). Regarding non-sensitive or pseudonymized patient data, individuals turned out to be indifferent in terms of acceptance of health clouds (F vs. G: t = -1.46 (-0.62), p-value = 0.1467 (0.5338); V = 3306.5 (1972), p-value = 0.1885 (0.3962)). Medical information sensitivity issues are regarded as important as timely delivery of medical records in formation of individuals' willingness (e.g., A vs. G: t = 1.68 (-1.56), p-value = 0.09395 (0.1198); V = 6000.5 (2515.5), p-value = 0.05405 (0.1706)). Individuals' acceptance of health clouds significantly falls when there are other options to deliver patient data. With regards to them, people do not significantly vary in their intentions towards health clouds (t = 0.71 (-0.75), p-value = 0.4767 (0.4519); V = 6435.5 (4133), p-value = 0.3127 (0.6547)).

	A	B	C	D	E	F
Individuals differ in their likeliness to approve to the transmission of their encrypted sensitive patient data over a cloud-based system (without (1st row) and with (2nd row) additional confidentiality through secret sharing), depending on whether …						
B	t = 10.47, p < 2.2e-16 V = 8915, p < 2.2e-16 t = 9.87, p < 2.2e-16 V = 6695.5, p < 2.2e-16					
C	t = -8.25, p = 7.817e-15 V = 2484, p = 2.994e-14 t = -7.50, p = 1.01e-12 V = 1524.5, p = 1.656e-12	t = -14.71, p < 2.2e-16 V = 994, p < 2.2e-16 t = -12.69, p < 2.2e-16 V = 977.5, p < 2.2e-16				
D	t = -5.71, p = 3.043e-08 V = 3127.5, p = 2.503e-08 t = -5.43, p = 1.294e-07 V = 2116.5, p = 1.341e-07	t = -12.59, p < 2.2e-16 V = 805, p < 2.2e-16 t = -11.44, p < 2.2e-16 V = 652.5, p < 2.2e-16	t = 3.83, p = 0.000162 V = 5941, p = 6.501e-05 t = 3.00, p = 0.002933 V = 3116, p = 0.001388			
E	t = -7.60, p = 5.245e-13 V = 2842, p = 1.518e-11 t = -7.52, p = 8.477e-13 V = 1540.5, p = 3.94e-12	t = -13.91, p < 2.2e-16 V = 940.5, p < 2.2e-16 t = -12.71, p < 2.2e-16 V = 362.5, p < 2.2e-16	t = 0.71, p = 0.4767 V = 6435.5, p = 0.3127 t = -0.75, p = 0.4519 V = 4133, p = 0.6547	t = -2.32, p = 0.02101 V = 4077, p = 0.02059 t = -2.75, p = 0.006367 V = 3107.5, p = 0.009232		
F	t = 3.03, p = 0.002718 V = 6460.5, p = 0.001107 t = -0.80, p = 0.4271 V = 3227, p = 0.5271	t = -5.58, p = 5.9e-08 V = 1704.5, p = 1.105e-08 t = -7.78, p = 1.638e-13 V = 1024, p = 5.418e-13	t = 11.53, p < 2.2e-16 V = 14519, p < 2.2e-16 t = 7.02, p = 1.852e-11 V = 8143, p = 5.151e-11	t = 7.98, p = 4.467e-14 V = 10666.5, p = 2.876e-13 t = 4.84, p = 2.171e-06 V = 6642.5, p = 1.569e-06	t = 11.0237, p < 2.2e-16 V = 11710, p < 2.2e-16 t = 7.5444, p = 7.427e-13 V = 7664.5, p = 1.437e-12	
G	t = 1.68, p =	t = -6.7767, p =	t = 8.89, p <	t = 6.10, p =	t = 9.32, p <	t = -1.46, p =

0.09395	8.042e-11	2.2e-16	3.865e-09	2.2e-16	0.1467
V = 6000.5, p = 0.05405	V = 1434.5, p = 1.301e-11	V = 14677, p = 1.066e-15	V = 10100.5, p = 9.784e-10	V = 11070.5, p = 2.753e-16	V = 3306.5, p = 0.1885
t = -1.56, p = 0.1198	t = -9.0036, p < 2.2e-16	t = 6.40, p = 6.948e-10	t = 4.26, p = 2.867e-05	t = 7.12, p = 1.052e-11	t = -0.62, p = 0.5338
V = 2515.5, p = 0.1706	V = 609.5, p < 2.2e-16	V = 8100.5, p = 1.487e-09	V = 7018, p = 8.95e-06	V = 6741, p = 6.776e-11	V = 1972, p = 0.3962

Table 25. Situation-Based Comparisons of Individuals' Acceptance of Health Clouds (see Table 24 for Abbreviations) (Grey: Supported; White: Not Supported)

7.5 Discussion

This study reveals that individuals are more eager to accept health clouds when being in an emergency situation. In non-emergency cases, the acceptance of health clouds is higher when they are used to transfer non-sensitive or pseudonymized patient data or when the timely delivery of patient data can otherwise not be guaranteed. These results confirm previous findings that there is a relatively high need among individuals to stay anonymous (Nass et al., 2009; Whiddett et al., 2006; Perera et al., 2011; Riordan et al., 2015) and conceal sensitive patient data (Zulman et al., 2011; Bansal et al., 2007, 2010) on the Internet. Without additional confidentiality assurances through secret sharing, concealing sensitive patient data is seen even more important than its timely delivery. Understandably, while medical records not timely delivered could result in repeated medical tests and/or delayed medical treatment (Ermakova et al., 2014a), disclosure of sensitive medical conditions could potentially destroy the individual's social status and employment opportunities (Bansal et al., 2010; Laric et al., 2009; Rohm and Milne, 2004; Cushman et al., 2010; Duquenoy et al., 2012; Appari and Johnson, 2010).

Individuals' acceptance of health clouds further decreases when sensitive medical records are sent by phone or brought by person. People are more likely to accept health clouds when their sensitive patient data is going to be transferred by a courier than when it can be telephonically sent or personally brought. Possibly, taxi is viewed as a less favourable and/or trustable transfer means than other considered options.

Finally, higher acceptance levels can be reached when additional confidentiality of sensitive patient data through secret sharing is provided. In fact, only in the case of non-sensitive medical records' transfer, individuals did not show any significant increase in their acceptance of health clouds when being guaranteed additional confidentiality through the mechanism. These results suggest that the willingness to accept health clouds for sharing sensitive health information varies depending on the level of offered confidentiality. The secret-sharing mechanism appears to make substantial guarantees. Moreover, as previously mentioned, concealing the sensitive part of medical data is not more preferred than its timely availability.

As in most empirical studies, the sample size used in this study was rather limited. Many of our subjects were rather young people who are probably more familiar with the cloud computing technology and may have had relatively few medical problems. Due to the reasons, it would be interesting to verify the findings of the present research with a more representative sample. Nevertheless, we were interested in examining whether and how individuals differed

in their likeliness to accept health clouds rather than describing an overall level of acceptance. Furthermore, the focus of this study was laid on the German-speaking society. In light of the possible globalization of the investigated application scenario, it would be beneficial to explore the relationships in other cultures. In addition, the cases presented could have appeared rather hypothetical to the participants. Experimental research with more detailed descriptions of the cases involved could be useful to replicate these study results. However, they reflect real situations which are rather time-critical. Future research may attempt to address these issues.

Following the suggestions by Streiner and Norman (2011), we do not correct for multiplicity to avoid type 2 errors as this study is rather aimed to discover fruitful areas of research.

7.6 Conclusion and Managerial Implications

Cloud computing can enable timely delivery of medical records to wherever they are needed. Nevertheless, as a result of individuals' concerns about potential confidentiality breaches and misuses of their health information, acceptance of cloud computing in healthcare might be at risk. While prior work reveals that individuals' concerns can be mitigated by persuading people about the efficacy of technological mechanisms to preserve their privacy, we investigated in this study whether the acceptance of health clouds can be increased through additional confidentiality assurances and whether it depends on a situational context. Based on over 260 full responses, we performed multiple t-tests and Wilcoxon signed rank tests for paired samples.

When asked about sensitive health information sharing under additional confidentiality assurances, participants were significantly more likely to accept health clouds. Moreover, individuals were made indifferent depending on the sensitiveness of medical data and its timely availability, while being otherwise rather privacy-oriented. In general, people show higher levels of willingness to accept health clouds for emergency cases. For non-emergency cases, health clouds can expect higher acceptance for delivery of non-sensitive or pseudonymized medical records and for delivery of sensitive medical records given the risk that they could not arrive in time otherwise. In the presence of casual offline transfer options (e.g., taxi), health clouds are less likely to get accepted, especially if the data can be sent by fax or brought by the patient personally.

Our findings lead to important implications for research and practice. Our paper provides a theoretical framework to measure individuals' acceptance of health clouds and calls for further research regarding privacy-preserving technological mechanisms. Healthcare providers wishing to profit from beneficial health clouds are provided with a number of possible courses of actions to make them seem more attractive to their patients. In general, this study shows that individuals' acceptance of health clouds could be strengthened with stronger confidentiality assurances regarding their health information. In particular, it can be done by cooperating with several independent cloud providers and applying the secret-sharing approach to encrypted medical records before sharing. With this approach, health clouds would become more popular among the supporters of casual offline transfer means. Moreover, healthcare providers could act as cloud providers themselves. To further boost health clouds' acceptance, healthcare providers can further offer their patients to remove their personal identifiers or exclude sensitive details from medical records. Recommendations on how to increase the acceptance of health clouds in every single case can be further worked out through data mining techniques.

8. Discussion

8.1 Promoting Trust

The study presented in Section 4 demonstrates that concerns for medical information privacy can be mitigated by building trust in privacy-preserving regulatory and technological mechanisms, and cloud providers in the healthcare sector. Luo and Najdawi (2004) argue that consumer health portals employ branding, self-regulating policies, ownership disclosure (as the owners are mainly major pharmaceutical companies, health maintenance organizations, or other for-profit organizations), source disclosure and third-party seals to build trust. The authors consider these measures to be effective in initiating one or more processes of building trust. These involve calculative, predictive, intentionality, capability and transference processes (see Table 26 for details and Section 2.3.3 for trust dimensions). The calculative process takes place when a trustor builds trust towards a trustee by previously estimating his or her costs and benefits to deceive or collaborate. The prediction process is observed when a trustor builds trust by predicting the trustee's future behavior based on his or her actions in the past. The intentionality process implies that trust is developed based on the perceived intentions of the trusted party. In the capability process, a trustor builds trust towards a trustee by evaluating his or her ability to fulfill promises, while the transference process means that trust towards an unknown entity is transferred from an already known one.

Process / Dimension	**Ability**	**Benevolence**	**Integrity**
Calculative			
Predictive	Branding	Branding	Branding
Intentionality		Self-regulating policies Ownership disclosure	Self-regulating policies
Capability	Source disclosure		
Transference	Branding Third-party seal Source disclosure	Branding Ownership disclosure	Branding Third-party seal

Table 26. Trust-Building Processes and Measures (Based on Luo and Najdawi (2004))

The presence of a privacy statement on a website was empirically shown to positively influence customers' trust towards the website (Jensen et al., 2005), as well as their beliefs about their privacy protection on the website (Li et al., 2011c), on the amount of personal information they were willing to disclose to the website (Hui et al., 2007), and intentions to purchase on the website (Jensen et al., 2005; Tsai et al., 2011) (Ermakova et al., 2015a; Ermakova et al., 2014b). Similarly, according to the US national phone survey, which was conducted by the Annenberg Public Policy Center in 2005, most Internet users believe that the presence of a privacy policy already means that the site will not share their personal information with third parties (Feldman et al., 2005) (Ermakova et al., 2015a).

Self-reported privacy statements which strongly guarantee security were shown to be more effective than third-party seals with regards to customers' willingness to disclose various types of personal information (Peterson et al., 2007). This finding implies that there is no necessity for investments in third-party seal programs. Nevertheless, the practice shows that Internet users only rarely read privacy policies (Acquisti and Grossklags, 2005; Acquisti, 2010; Jensen et al., 2005) and rely on third-party seals instead (Milne and Culnan, 2004). Empirical evidence demonstrates that individuals consult privacy policies only in 26% of cases where they are available (Jensen et al., 2005). Similarly, 77% of a Facebook's study participants had not read the company's privacy policy (Acquisti and Gross, 2006). (Ermakova et al., 2015a)

People's reading of privacy policies and trust in the notice can be impacted by perceived comprehension of privacy notices (Milne and Culnan, 2004). The readability of a privacy statement was even found to be positively associated with users' trust towards the website (Ermakova et al., 2014b; Sultan et al., 2002; Bansal et al., 2008a, 2008b; Antón et al., 2007). Studies indicate that many privacy policies suffer from a lack of readability (Graber et al., 2002; McDonald et al., 2008, 2009; Sunyaev et al., 2014; Ermakova et al., 2015a), do not address users' privacy concerns (Pollach, 2007) and do not even focus on the service at all (Sunyaev et al., 2014). (Ermakova et al., 2015a)

8.2 Searching for a Rigorous Model of Health Clouds Acceptance

8.2.1 Privacy Awareness

The study presented in Section 4 did not find support for the hypothesis that knowledge about information privacy, both stated and actual, exerts a significant impact on information privacy concerns in the health cloud scenario. On the contrary, privacy concerns were found to be negatively affected by Internet literacy (Dinev and Hart, 2006b) and Internet technical literacy (Dinev and Hart, 2004; Brecht et al., 2012), and positively influenced by social awareness (Dinev and Hart, 2004, 2006b) and privacy awareness (Brecht et al., 2012) (see Section 2.3.4 for details). Richards (2012) similarly reveals a statistically significant difference in the level of privacy concern between groups based on education level (Richards, 2012, p. 121), with higher educated individuals having higher means (Richards, 2012, p. 147). As argued by Dinev and Hart (2006b), the more Internet literacy users have, the more competent they perceive themselves with regards to their privacy protection and the less concerned they are about their privacy. Internet users with higher social awareness presumably tend to know more about privacy issues and therefore to be more concerned about their privacy.

Furthermore, behavioral intention to transact online was also shown to be negatively influenced by Internet literacy (Dinev and Hart, 2005, 2006b) and technology awareness (Dinev and Hu, 2005, 2007).

Finally, Ancker et al. (2012) revealed that individuals with a high school education or less were less likely to believe that HIE would improve healthcare quality. Richards (2012) similarly confirms a statistically significant difference in the level of perceived usefulness of electronic PHR between groups based on education level (Richards, 2012, p. 122), with higher educated individuals having higher means (Richards, 2012, p. 148).

8.2.2 Control Variables

TNS Emnid (2009) found that trust in Internet decreased with age. Richards (2012) also observes a statistically significant difference in the level of disposition in trust, institution-based trust ("*perceptions of the Internet environment*"), trusting beliefs ("*perceptions of specific Web vendor attributes*"), and trusting intentions ("*intention to engage in trust-related behaviors with a specific Web vendor*") between groups based on age (Richards, 2012, pp. 26, 117-118). However, in the study by Rauer (2012), the relationship between age and overall trust in Internet-based health records turned out to be not significant.

In the study by Richards (2012), females had higher means for intention to access, manage, share an ePHR with healthcare providers, public healthcare facilities, third-party payers as well as use it as an authorized representative of a third party (Richards, 2012, pp. 143-144), although the differences between the gender responses for these construct were found statistically insignificant, except for intention to share with third-party payers (Richards, 2012, p. 115).

8.2.3 Research Method

To elaborate on these issues, recent criticism on performing SEM studies should be taken into account. As stated by Zheng and Pavlou (2010), in most SEM studies researchers specify just one model structure and use data to confirm or disconfirm it, whereas equivalent models are potentially overlooked due to the lack of an automated method for exploring alternative models. Sharma and Kim (2012) observe the tendency to select unnecessarily complex models being far from reality and thus hardly interpretable. Moreover, being additionally flexible, complex models may rather imitate sample specific patterns and thus poorly generalize to other samples (Myung, 2000; James, 2013, pp. 239-241). Finally, as Gefen et al. (2011) argues, PLS research reports rarely compare the hypothesized theoretical model with the saturated model, where all possible paths are included, in order to make sure that the paths being significant in the theoretical model are significant in the saturated model, as well.

Specifically, subset selection can be applied to the considered problem, which, along with shrinkage (also known as regularization), dimension reduction and other approaches, represents a well-established class of methods to fit least squares (James, 2013, p. 204, Hastie et al., 2009, p. 57). The methods for selecting subsets of predictors include best model selection and stepwise selection procedures (James, 2013, p. 205). These procedures can be conducted following the instructions by James (2013, pp. 205-207, 210-214, 244-251), Fox and Weisberg (2011, p. 213), Hastie et al. (2009, pp. 57-58) and James (2013, pp. 207-214), Dalgaard (2002, pp. 154-157), Fox and Weisberg (2011, pp. 207-213), Hastie et al. (2009, pp. 58-60), respectively.

In the ordinary least squares framework which PLS rests on, the problem of model selection is often related to selection of variables: Given a response y and a set of predictors $x=\{x_1, \ldots, x_m\}$, our goal is to divide x into the groups of active and inactive predictors, $x=(x_A, x_I)$, so that $y|x_A$ (i.e., y given x_A) is distributed the same as $y|(x_A, x_I)$, e.g., in simple words, the active predictors contain all the information about y (Fox and Weisberg, 2011, pp. 207-213; James et al., 2013, p. 204; Fan and Lv, 2010). When irrelevant variables are removed, the resulting model can be more easily interpreted (James et al., 2013, p. 204; Fan and Lv, 2010). However, James et al. (2013, p. 204) state that it would be extremely unlikely that least squares yield any coefficient estimates being exactly zero. Traditional measures such as R^2 statistics should

also not be used to judge the quality of models with different subsets of predictors (James, 2013, pp. 243-244). It can be easily shown that the model R^2 increases to 1 whenever extra predictors, which are even completely unrelated to the response, are included into the model (James et al., 2013, pp. 240-241; Sharma and Kim, 2012). The more recommended statistics (or model selection criteria) include Akaike information criterion (AIC), Mallow's Cp, Bayesian information criterion (BIC), and adjusted R^2, etc. which correct for the increase in model complexity (James et al., 2013, p. 78). In the study by Sharma and Kim (2012), these and other model selection criteria were tested in the PLS context. For a sample size of 250 which is similar to our settings, adjusted R^2, Cp, AIC and BIC achieved correct identification rates of 49%, 59%, 59% and 56%, respectively. With R squared, only 3% of the models were correctly identified. Further important results can be reported if measured on an independent test set. For the validation set approach, the observations are split into a training set and a test set. Models are built based on the training set, while the model with the smallest resulting prediction error measured on the test set is selected (James, 2013, pp. 213-214, 243-244).

It is further worth discussing in which situations best subset selection and stepwise selection should be applied. There are a total of 2 to the power of p models that contain subsets of p variables (James et al., 2013, p. 78). When p is rather small so that all models can be considered, best subset selection is usually preferred: First, the algorithm builds all models for each possible number of predictors ranging from 1 until the number of all possible predictors. It further chooses the best model among the models with a given number of predictors. Finally, the algorithm selects a single best model (James et al., 2013, p. 205). When p is rather large, so that not all models could be considered, stepwise selection is usually applied which is offering three choices. The "backward" procedure implies that the start model contains all possible predictors. All models where one of the predictors is removed are then built and the best one among them is chosen. In the final step, a single best model is selected. The "forward" stepwise selection algorithm starts with the model that contains no predictors and builds further models by augmenting the predictors with one additional predictor. The "both" procedure considers both an addition and a removal. (Fox and Weisberg, 2011, pp. 207-213; James et al., 2013, pp. 78-79, 209)

8.3 Understanding Physicians' Adoption of Health Clouds

The study presented in Section 4 considered only a patient perspective. However, Simon et al. (2007) argue that physicians are worried about patient privacy even more than the patients themselves.

Title	Understanding Physicians' Adoption of Health Clouds
Authors	Ermakova, Tatiana, Technical University of Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, tatiana.ermakova@tu-berlin.de
Published in	Proceedings of the 4th International Conference on Information Technology Convergence and Services (ITCS 2015) (Ermakova, 2015)
Abstract	Recently proposed health applications are able to enforce essential advancements in the healthcare sector. The design of these innovative solutions is often enabled through the cloud computing model. With regards to this technology, high concerns about information security and privacy are common in practice. These concerns with respect to sensitive medical information could be a hurdle to successful adoption and consumption of cloud-based health services, despite high expectations and interest in these services. This research attempts to understand behavioural intentions of healthcare professionals to adopt health clouds in their clinical practice. Based on different established theories on IT adoption and further related theoretical insights, we develop a research model and a corresponding instrument to test the proposed research model using the partial least squares (PLS) approach. We suppose that healthcare professionals' adoption intentions with regards to health clouds will be formed by their outweighing two conflicting beliefs which are performance expectancy and medical information security and privacy concerns associated with the usage of health clouds. We further suppose that security and privacy concerns can be explained through perceived risks.
Keywords	Cloud Computing, Healthcare, Adoption, Physician, Security and Privacy Concerns

8.3.1 Introduction

Nowadays, healthcare and medical service delivery are on the way to be revolutionized (BMWi, 2015; Hardesty, 2013). Due to the recently proposed solutions, medical data can be easily shared and collaboratively used by healthcare professionals involved in the medical treatment (TRESOR, 2015), while novice surgeons can automatically be assisted in their surgical procedures (Mani and Li, 2013) and physicians can be supported to make their therapy-related decisions (Lupse et al., 2013). The design of these apparently important innovative healthcare solutions is often enabled through the cloud computing model, which is known for providing adequate computing and storage resources on demand (Mell and Grance, 2012). However, the immediate involvement of the cloud computing's third-party as well as communication via the open Internet landscape might lead to unexpected risks (e.g., legal problems) (Boonstra and Broekhuis, 2013; Najaftorkaman and Ghapanchi, 2014) and therefore cause intense concerns among medical workers with respect to cloud computing companies' ability and willingness to protect disclosed medical information (Ion et al., 2011; Opitz et al., 2012; TRUSTe, 2015). While online medical service providers currently show interest in collecting medical information of their customers (Huesch, 2013; Kaletsch and Sunyaev, 2011), through the misuse of medical information the service users might get subject to harassment by marketers of medical products and services, and discrimination by employers, healthcare insurance agencies, and associates (Bansal et al., 2010; Laric et al., 2009). The exposure of security and privacy concerns related to sensitive medical information could be a serious hurdle to successful adoption and consumption of cloud-based health services, as repeatedly demonstrated by prior empirical evidence in other healthcare settings (Angst and Agarwal, 2009; Bansal et al., 2007, 2010; Ermakova et al., 2014a; Dinev et al., 2012; Lian et al., 2014; Boonstra and Broekhuis, 2013; Najaftorkaman and Ghapanchi, 2014; Bassi et al., 2012).

This research examines which determinants can explain the extent to which medical workers will be willing to adopt health clouds in their daily work. To conduct the research, we follow the guidelines proposed by Urbach and Ahlemann (2010), Petter et al. (2007), MacKenzie et al. (2011), and Gefen et al. (2000). We build on well-established theories and works on adoption of information technologies (Venkatesh et al., 2003; Venkatesh et al., 2012) and existing theoretical insights into the factors influencing healthcare IT and cloud computing adoption. We further draw on utility maximization theory (Bansal et al., 2010; Dinev and Hart, 2006a) arguing that one tries to maximize his or her total utility. We suppose the utility function to be given by the trade-off between expected positive and negative outcomes in a healthcare professional's decision-making process with regards to the usage of health clouds.

The paper is divided into four sections. In Section 8.3.2, we introduce the background of our research, highlight main theoretical foundations and formulate research hypothesis. Section 8.3.3 proceeds with presenting the research model where we illustrate the hypothesized relations. It further deals with the instrument developed to test the proposed research model using the partial least squares (PLS) approach (Gefen et al., 2000, 2011; Urbach and Ahlemann, 2010). We conclude by recapitulating the results of this work, extensively discussing its limitations and thus giving recommendations for further research.

8.3.2 Background and Theoretical Foundations

The availability of medical data is of utmost importance to physicians during the medical service delivery (TRESOR, 2015). The healthcare sector can further profit from modern data analysis techniques. Their application fields in the healthcare area range from disease detec-

tion, disease outbreak prediction, and choice of a therapy to useful information extraction from doctors' free-note clinical notes, and medical data gathering and organizing Hardesty, 2013. These techniques can also be applied to assessment of plausibility and performance of medical services and medical therapies development (BMWi, 2015). Recently, Mani and Li (2013) introduced an interactive three-dimensional e-learning portal for novice surgeons. Under real time conditions, their surgical procedures are to be compared to the practice of experienced surgeons. Lupse et al. (2013) presented a decision support system aimed to assist physicians in finding a successful treatment for some certain illness based on the currently available best practices and the characteristics of a given patient.

By provisioning adequate capacities to store and process huge amounts of data, cloud computing facilitates the design of these innovative applications in the healthcare area. However, this technology is also known for users' concerns about their information security and privacy (Ion et al., 2011; Opitz et al., 2012). While the providers of healthcare-related websites are interested in collecting medical information (Huesch, 2013; Kaletsch and Sunyaev, 2011), the misuse of medical information might result in different harassment and discrimination scenarios for patients (Bansal et al., 2010; Laric et al., 2009). In the recent past, there were cases where, based on disclosed medical information, marketers of medical products and services sent their promotional offers; employers refused to hire applicants and even fired employees; insurance firms denied life insurances. The exposure of the concerns surrounding information security and privacy could therefore negatively affect adoption and consumption of cloud-based health services, as multiple empirical studies demonstrated this in the healthcare context (Angst and Agarwal, 2009; Bansal et al., 2007, 2010; Ermakova et al., 2014a; Dinev et al., 2012; Lian et al., 2014; Boonstra and Broekhuis, 2013; Najaftorkaman and Ghapanchi, 2014; Bassi et al., 2012) and other settings (Dinev and Hart, 2006a, 2006b; Smith et al., 1996).

In the present work, we try to understand the predictors of behavioural intention of healthcare professionals to adopt health clouds in their work. In the research related to management of information systems (MIS), a variety of theories have been applied to explain an individual's adoption of information technologies. Among others, these include theories of reasoned action (TRA), planned behaviour (TPB), technology acceptance model (TAM), and unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003, 2012). In line with these theories, we suppose that healthcare professionals' adoption of health clouds is a product of beliefs surrounding the system. We additionally assume that medical workers' intentions are consistent with utility maximization theory (Bansal et al., 2010; Dinev and Hart, 2006a) which posits that an individual attempts to maximize his or her total utility. As usage of health clouds is associated with numerous risks for a healthcare professional, we suppose that his or her utility function in the presented context is given by the calculus of conflicting beliefs which involve performance expectancy of the services, on one side, and associated security and privacy concerns about medical information, on the other side. We further postulate that information security and privacy concerns result from perceived risks.

8.3.2.1 Performance Expectancy

In one of the recent works on information technology acceptance, Venkatesh et al. (2003) defines performance expectancy as the extent to which individuals believe that using the information technology is helpful in attaining certain gains in their job performance. Performance expectancy and other factors that pertain to performance expectancy such as perceived usefulness are generally shown to be the strongest predictors of behavioural intention (Venkatesh et al., 2003). Previous work suggests that healthcare professionals tend to be higher willing to

adopt technological advances in their practice the higher they perceive their usefulness (Dünnebeil et al., 2012; Chau and Hu, 2001; Vathanophas and Pacharapha, 2010; Najaftorkaman and Ghapanchi, 2014). Similarly, cloud computing is more likely to be adopted the more beneficial it appears to the decision maker (Hsu et al., 2014; Li and Chang, 2012; Lian et al., 2014; Opitz et al., 2012). Therefore, we hypothesize that:

Hypothesis 1. Performance expectancy will be positively associated with behavioural intention to accept health clouds.

8.3.2.2 Security and Privacy Concerns

Online companies rely on use of their customers' personal information to select their marketing strategies (Opitz et al., 2012; Kaletsch and Sunyaev, 2011). As a result of this, Internet users view their privacy as being invaded. A recent survey revealed that 90% of Americans and Britons felt concerned about their online privacy and over 70% of Americans and 60% of Britons were even higher concerned than in the previous year (TRUSTe, 2015).

Healthcare professionals appear to be ones of the most anxious Internet users in terms of information privacy. Dinev and Hart (2006b) argue that Internet "users with high social awareness and low Internet literacy tend to be the ones with the highest privacy concerns". Although this group of users constitute the intellectual core of society, they are not able or willing to keep up with protecting technologies while using the Internet. Simon et al. (2007) further state that physicians are worried about patient privacy even more than the patients themselves.

In this study, privacy concerns are related to healthcare professionals' beliefs regarding cloud computing companies' ability and willingness to protect medical information (Smith et al., 1996; Bansal, 2011b; Opitz et al., 2012). The dimensions of privacy concerns involve errors, improper access, collection, and unauthorized secondary usage.

Due to the open Internet infrastructure vulnerable to multiple security threats (Opitz et al., 2012), we further consider security concerns. They refer to healthcare professionals' beliefs regarding cloud computing companies' ability and willingness to safeguard medical information from security breaches (Bansal, 2011b; Opitz et al., 2012). The dimensions of security concerns include information confidentiality and integrity, authentication (verification) of the parties involved and non-repudiation of transactions completed.

Similarly to Bansal (2011b), we distinguish six dimensions of the combined security and privacy concerns, where we consider the dimensions of errors and improper access to be equivalent to the dimension of integrity and confidentiality, respectively (see Figure 13).

Multiple empirical studies repeatedly confirm that individuals' privacy concerns reduce behavioural intentions in a variety of settings (Angst and Agarwal, 2009; Bansal et al., 2007, 2010; Dinev and Hart, 2006b; Dinev et al., 2006a; Ermakova et al., 2014a; Smith et al., 1996). Business concerns involving confidentiality were shown to negatively affect one's intention to adopt cloud computing (Hsu et al., 2014). Information privacy and security are among the most influential factors of technology adoption decisions made in hospitals (Lian et al., 2014; Boonstra and Broekhuis, 2013; Najaftorkaman and Ghapanchi, 2014; Bassi et al., 2012). Therefore, we argue that:

Hypothesis 2. Security and privacy concerns will be negatively associated with behavioural intention to accept health clouds.

8.3.2.3 Perceived Risks

Various laws and regulations such as Directive 95/46/EC of the European Parliament and of the Council (European Parliament and Council, 1995) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) (U.S. Department of Health and Human Services, 2015) determine how personal medical information is to be handled. When violations occur, healthcare professionals might experience legal problems as a result of medical information disclosure to health clouds, as well (Boonstra and Broekhuis, 2013; Najaftorkaman and Ghapanchi, 2014). Similar to Dinev et al. (2013), we define perceived risk as the extent to which a healthcare professional expects to suffer a negative outcome as a consequence of usage of the services. Empirical evidence demonstrates that the higher he or she perceives the vulnerabilities and risks associated with the usage of certain services (Dinev and Hart, 2004, 2006a; Dinev et al., 2006a; Dinev et al., 2013; Xu et al., 2008; Xu et al., 2011), the higher one is concerned about information privacy. This finding was also found applicable in the cloud computing adoption setting, with respect to security and privacy concerns (Li and Chang, 2012). Therefore, we postulate that:

Hypothesis 3. Perceived risks will be positively associated with security and privacy concerns.

8.3.3 Model Construction and Instrument Development

In this work, we theorize that two constructs will be significant direct determinants of acceptance of health clouds among medical workers. These include performance expectance and security and privacy concerns. As previously explained, we further suppose that security and privacy concerns will result from perceived risks (see Figure 13).

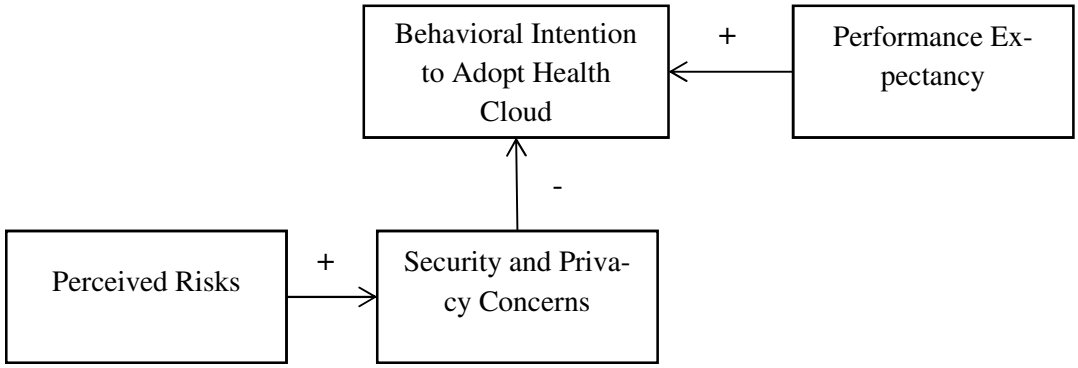

Figure 13. Research Model

Table 27 presents the questionnaire items to measure the research model constructs. We developed the scales based on a comprehensive literature survey. All construct measures are reflective, i.e., they share a similar content and are affected by the changes in the construct they measure (Petter et al., 2007; Urbach and Ahlemann, 2010). Behavioural intention to adopt health clouds and performance expectancy are to be measured with items adapted from Venkatesh et al. (2003, 2012). Security and privacy concerns are to be explored at a more de-

tailed level, as recommended by Angst and Agarwal (2009). With regards to the concerns, we draw on the multi-dimensional view proposed by Bansal (2011b). The dimensions of privacy-related concerns, i.e., collection, errors, unauthorized secondary use, and improper access, originate from the work by Smith et al. (1996) and were validated in healthcare privacy studies (Dinev et al., 2012; Ermakova et al., 2014a). To measure the factors associated with collection, integrity/errors, and confidentiality/improper access, the questions from Ermakova et al. (2014a) were adapted. For the secondary use construct, we took items from Dinev and Hart (2006a). Measures for the remaining underlying factors, i.e., authentication and non-repudiation, were developed based on Bansal (2011b). To measure perceived risks, we rely on the items by Dinev et al. (2013).

Construct	**Items**
Behavioural Intention to Adopt Health Clouds (based on Venkatesh et al., (2003, 2012))	Given I get the system offered in the future and the patient consent for medical information transmission over the system is given, … … I intend to use it whenever possible. … I plan to use it to the extent possible. … I expect that I have to use it.
Performance Expectancy (based on Venkatesh et al., (2003, 2012))	Using the system would make it easier to do my job. I would find the system useful in my job. If I use the system, I will spend less time on routine job tasks.
Security and Privacy Concerns – Integrity / Errors (based on Bansal (2011b), Smith et al. (1996), Ermakova et al. (2014a))	I would be concerned that in the system… … medical information can be modified (altered, corrupted). … medical information is not enough protected against modifications. … accurate medical information can hardly be guaranteed.
Security and Privacy Concerns – Confidentiality / Improper Access (based on Bansal (2011b), Smith et al. (1996), Ermakova et al. (2014a))	I would be concerned that in the system… … medical information can be accessed by unauthorized people. … medical information is not enough protected against unauthorized access. … authorized access to medical information can hardly be guaranteed.
Security and Privacy Concerns – Authentication (based on Bansal (2011b))	I would be concerned that in the system… … transactions with a wrong user can take place in the system. … verifying the truth of a user in the system is not enough ensured. … transacting with the right user in the system can hardly be guaranteed.
Security and Privacy Concerns – Nonrepudiation (based on Bansal (2011b))	I would be concerned that transactions in the system … …. could be declared untrue. … are disputable. … are deniable.
Security and Privacy Concerns – Collection (based on Bansal (2011b), Smith et al. (1996), Ermakova et al. (2014a))	I would be concerned that medical information transmitted over the system … … does not get deleted from the cloud. … is kept as a copy. … is collected by the cloud provider.

Security and Privacy Concerns – Unauthorized Secondary Use (based on Bansal (2011b), Smith et al. (1996), Dinev and Hart (2006a))	I would be concerned that medical information transmitted over the system can be … … used in a way I did not foresee. … misused by someone unintended. … made available/sold to companies or unknown parties without your knowledge.
Perceived Risks (based on Dinev et al. (2013))	In general, it would be risky to transmit medical information over the system. Transmitting medical information over the system would involve many unexpected problems. I would not have a good feeling when transmitting medical information over the system.

Table 27. Research Model Constructs and Related Questionnaire Items

The respondents are supposed to be presented one of the above mentioned scenarios. They further will be asked to provide their answers to the questions on a 7 Likert scale (e.g., 1: Not likely at all, 2: Highly unlikely, 3: Rather unlikely, 4: Neither likely nor unlikely, 5: Rather likely, 6: Highly likely, 7: Fully likely). Additionally, they will be asked about practice period (DesRoches et al., 2008), their workplace location (e.g. rural or urban) (Najaftorkaman and Ghapanchi, 2014; DesRoches et al., 2008), gender, and age, etc. (Najaftorkaman and Ghapanchi, 2014). These questions will mainly allow describing the sample.

8.3.4 Conclusion, Limitations and Suggestions for Future Research

In this work, we defined a theoretical model aimed to explain behavioural intention of healthcare professionals to adopt health clouds in their clinical practice. We operationalized the research model and transferred it into a structural equation model to further analyse with the PLS approach.

Drawing on utility maximization theory and further related research, we suppose that healthcare professionals' adoption intentions with regards to health clouds will be formed by outweighing two conflicting beliefs. They involve expected performance expectancy and security and privacy concerns associated with the usage of health clouds. We further postulate that security and privacy concerns can be explained through perceived risks.

Our work implies some limitations. First, there might be some other possible casual relationships between the constructs proposed in the research model. For example, Vathanophas and Pacharapha (2010) hypothesize that EMR security/confidentiality influences its perceived usefulness, while Dünnebeil et al. (2012) find a positive relationship between perceived importance of data security and perceived usefulness of electronic health services. As identified by Krasnova et al. (2009), perceived privacy risk directly influences personal information disclosure in the context of online social networks. In our future research, we are going to verify all possible paths, as recommended by Gefen et al. (2011).

Second, we left some other factors out of consideration such as effort expectancy, social influence, and facilitating conditions which are often investigated and can extend the study in the future.

Venkatesh et al. (2003) define effort expectancy as referring to the extent to which an individual finds the system easy to use. The factor is also captured by perceived ease of use specified in TAM. Perceived ease of use is important for potential cloud computing users (Li and Chang, 2012; Opitz et al., 2012). Physicians view easy-to-use services as more useful and stronger intend to use them (Dünnebeil et al., 2012; Boonstra and Broekhuis, 2013; Najaftorkaman and Ghapanchi, 2014). Contrary to these findings and other previous research assertions (e.g., Venkatesh et al., 2003, 2012), perceived ease of use did not exert any significant effects on perceived usefulness or attitude, when tested in the telemedicine context (Chau and Hu, 2001). The authors suggest that physicians comprehend new information technologies more easily and quickly than other user groups do. Alternatively, the importance of perceived ease of use may be weakened by increases in general competence or staff assistance (Chau and Hu, 2001). These aspects are implied in the concept of facilitating conditions which relates to the extent to which individuals believe in the existence of an organizational and technical infrastructure to support their system use (Venkatesh et al., 2003). They were found to play a role in formation of behavioural intention to use cloud computing in hospital (Lian et al., 2014) and perceived usefulness of healthcare information technologies (Chau and Hu, 2001; Moores, 2012; Boonstra and Broekhuis, 2013; Najaftorkaman and Ghapanchi, 2014).

Social influence refers to the degree to which individuals perceive that others' beliefs about their system use are important (Venkatesh et al., 2003). Being differently labelled across studies, social influence was found to have contradictory results when tested with regards to behavioural intention. Cloud computing users were significantly guided by the way they believe they are viewed by others as having used the cloud computing technology (Li and Chang, 2012). However, practicing physicians' intentions to use telemedicine technology were not significantly influenced by social norms (Chau and Hu, 2001). Dinev and Hu (2005) observe subjective norm influencing behavioural intention rather for IT aware groups. Dinev and Hu (2005) believe that the more IT knowledgeable the group are, the more they communicate about IT related issues and are willing to learn IT solutions their peers already use.

Finally, some variables which are to be used to describe the sample (e.g., workplace location) can further be controlled for their role. As observed by Najaftorkaman and Ghapanchi (2014), urban hospitals could be expected to adopt innovative solutions rather than rural ones. Hospitals located outside cities and towns are the only alternative for people living nearby. So they do not have to compete with others in adopting new technologies. Furthermore, they are typically under-occupied and have little financial support.

9. Conclusion

Applied to the area of healthcare, cloud computing has drawn tremendous interest in the research. There are multiple proposals to be employed in emergency healthcare, home healthcare, assistive healthcare, and telemedicine, as well as generally aimed at storage, sharing and processing of large medical resources.

Researchers argue that cloud computing enables availability, accessibility, recovery and transfer of medical resources. Furthermore, it is also believed to facilitate storage, management, search, processing and analysis of medical resources. In addition, cloud computing is associated with enabled connection, coordination, collaboration, and communication between medical staff (both within one medical institution and across multiple ones), patients, and other related parties in the healthcare area. Finally, the paradigm is expected to reduce construction, adoption and maintenance expenditures in healthcare.

Through an extensive literature review, this research particularly reveals that there is still a need for further development and improvement of the existing security and privacy-preserving mechanisms for health clouds, whereas related security and privacy concerns are viewed as an important barrier to their employment. So this research further examines the role of health information privacy concerns in the formation of individuals' acceptance of health clouds. The findings provide empirical support for the privacy calculus theory, what implies that perceived benefits and patient information privacy concerns actually compete in their impact on individuals' acceptance of health clouds; however, the effect of personal interest is shown to prevail.

Furthermore, this research tests the importance of trust in privacy-preserving regulatory and technological mechanisms and cloud providers in healthcare, as well as both stated and actual awareness about information privacy; only the impact of the latter three factors was confirmed. In a separate study, it could be repeatedly demonstrated that stronger confidentiality measures and assurances can actually result in increased acceptance of health clouds among individuals. To verify this positive influence and support the acceptance process, important security and privacy system requirements were deduced and addressed in the design of a multi-cloud provider architecture. Apart from classical encryption and other security measures, this architecture incorporates a secret-sharing mechanism to disseminate medical records as fragments to different cloud providers, therefore protecting patient privacy even in the case of compromised encryption keys or broken or insecurely implemented encryption algorithms. Under these confidentiality assurances, individuals are shown to be significantly more likely to accept health clouds for medical workers' sharing sensitive health information.

The present research leads to important theoretical and practical implications. It provides a comprehensive theoretical framework to understand the formation of both individuals' medical information privacy concerns and acceptance of health clouds. It supports the call for further improvements of technologies preserving security and privacy. One of the important practical lessons suggested by this research implies that healthcare providers may have means to actively manage their patients' privacy concerns and acceptance of health clouds. Trust-building actions should be undertaken towards privacy-preserving regulatory and technological mechanisms, and cloud providers in the healthcare sector. Despite present concerns for health information privacy, a higher level of acceptance can be ensured through convincing individuals of their benefits through health clouds or/and further strengthening those benefits. Furthermore, personal identifiers and sensitive details should be excluded from medical rec-

ords. For sensitive medical records, the application of the proposed multi-cloud provider architecture would also lead to higher support of health clouds.

This work has several limitations which open up new interesting avenues for future explorations. First, there might be some other possible relationships between the constructs in the theoretical model which were left out of consideration in the present research. Further research should therefore investigate other equivalent model structures. Future effort could be directed at measuring other beliefs related to individuals' medical information privacy concerns and acceptance of health clouds. Important contributions can also be made regarding the ways to encourage trust in the context of health clouds. Second, though our sample size was large enough to derive statistically rigorous and valid conclusions, it would be of interest to expand it to make broad statements about society in the German-speaking area, some other region and as a whole. Third, the measures used in this research capture high levels of their constructs, given the general focus of our study. However, researchers should attempt to confirm the empirical results of this thesis using other measures or research strategies. For example, the focus can be set on particular cloud computing offerings in the healthcare area. Fourth, this work initiates research related to adoption of health clouds from the perspective of medical workers and proposes a theoretical model to test. Finally, this work demonstrates experimental results with respect to Shamir's secret-sharing scheme and Rabin's information dispersal algorithm. Their low computational overhead is a good indicator for the feasibility of the proposed architecture. In the future, its further enhancement, full implementation, and validation of its deployment in real world settings should be strived for.

10. References

Abbadi, I.M.; Deng, M.; Nalin, M.; Martin, A.; Petkovic, M.; Baroni, I.: Trustworthy Middleware Services in the Cloud. 3rd International Workshop on Cloud Data Management (CloudDB), 2011.

Abbas, A.; Khan, S.U.: A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds. IEEE Journal of Biomedical and Health Informatics 18 (2014), 4, pp. 1431-1441.

Acquisti, A.; Gross, R.: Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. 6th International Conference on Privacy Enhancing Technologies (PET), 2006.

Andriole, S.J.: Seven Indisputable Technology Trends That Will Define 2015. Communications of the Association for Information Systems 30 (2012), pp. 61-72.

Ahuja, S.P.; Mani, S.; Zambrano, J.: A Survey of the State of Cloud Computing in Healthcare. Network and Communication Technologies 1 (2012), 2, pp. 12-19.

Ajzen, I.: The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes 50 (1991), 2, pp. 179–211.

Ajzen, I.; Fishbein, M.: Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood-Cliffs, New Jersey, 1980.

Altman, I.: The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Brooks/Cole Pub. Co., Monterey, California, 1975.

Ancker, J.S.; Silver, M.; Miller, M.C.; Kaushal, R.: Consumer Experience with and Attitudes toward Health Information Technology: a Nationwide Survey. American Medical Informatics Association 20 (2012a), 1, pp. 152–156.

Ancker, J.S.; Edwards, A.M.; Miller, M.C.; Kaushal R.: Consumer Perceptions of Electronic Health Information Exchange. American Journal of Preventive Medicine 34 (2012b), 1, pp. 76-80.

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 (2009), 2, pp. 339-370.

Andress, J.: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress, 2014.

Antón, A.I.; Bertino, E.; Li, N.; Yu, T.: A Roadmap for Comprehensive Online Privacy Policy Management. Communications of the ACM 50 (2007), 7, pp. 109-116.

Appari, A.; Johnson, M.E.: Information Security and Privacy in Healthcare: Current State of Research. International Journal of Internet and Enterprise Management 6 (2010), 4, pp. 279-314.

Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A. D.; Katz, R. H.; Konwinski, A.; Lee, G.; Patterson, D. A.; Rabkin, A.; Stoica, I.; Zaharia, M.: Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, University of California, Berkeley, 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf. Accessed on October 21, 2014.

Asmuth C.; Bloom, J.: A Modular Approach to Keysafeguarding. IEEE Transactions on Information Theory 29 (1983), 2, pp. 208–210.

Bansal, G.; Zahedi, F.; Gefen, D.: The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online. 13th Americas Conference on Information Systems (AMCIS), 2007.

Bansal, G.; Zahedi, F.; Gefen, D.: The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation. 30th International Conference on Information Systems (ICIS), 2008a.

Bansal, G.; Zahedi, F.; Gefen, D.: Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online. 14th Americas Conference on Information Systems (AMCIS), 2008b.

Bansal, G.; Davenport, R.: Moderating Role of Perceived Health Status on Privacy Concern Factors and Intentions to Transact with High versus Low Trustworthy Health Websites. 5th MWAIS (Midwest Association for Information) Conference, 2010.

Bansal, G.; Zahedi, F.: Trading Trust for Discount: Does Frugality Moderate the Impact of Privacy and Security Concerns? 16th Americas Conference on Information Systems (AMCIS), 2010.

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

Bansal, G.: Security Concerns in the Nomological Network of Trust and Big 5: First Order Vs. Second Order. 33th International Conference on Information Systems (ICIS), 2011a.

Bansal, G.: Understanding the Security in Privacy-Security Concerns: A Theoretical and Empirical Examination. 17th Americas Conference on Information Systems (AMCIS), 2011b.

Bansal, G.: Unauthorized Information Sharing Vs. Hacking: The Moderating Role of Privacy Concern on Trust Found and Lost. 18th Americas Conference on Information Systems (AMCIS), 2012.

Bassi, J.; Lau, F.; Lesperance, M.: Perceived Impact of Electronic Medical Records in Physician Office Practices: A Review of Survey-Based Research. Interactive Journal of Medical Research 1 (2012), 2, p. e3.

Basu, S.; Karp, A.; Li, J.; Pruyne, J.; Rolia, J.; Singhal, S.; Suermondt, J.; Swaminathan, R.: Fusion: Managing Healthcare Records at Cloud Scale. IEEE Computer Special Issue on Move Toward Electronic Health Records 45 (2012), 11, pp. 42-49.

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

Berndt, R-D.; Takenga, M.C.; Kuehn, S.; Preik, P.; Sommer, G.; Berndt, S.: SaaS-Platform for Mobile Health Application. 9th IEEE International Multi-Conference on Systems, Signals and Devices (IEEE SSD), 2012.

Bessani, A.N.; Correia, M.P.; Quaresma, B.; Andre, F.; Sousa, P.: Depsky: Dependable and Secure Storage in a Cloud-of-Clouds. 6th European Conference on Computer Systems (EuroSys), 2011.

Blakley, G.: Safeguarding Cryptographic Keys. AFIPS National Computer Conference, 1979.

Beimel, A.: Secure Schemes for Secret Sharing and Key Distribution. PhD Thesis, Israel Institute of Technology, Israel, 1996.

BCS: BCS Data Guardianship Survey, 2008. http://www.bcs.org/upload/pdf/dgs2008.pdf. Accessed February 5, 2015.

BMWi (Bundesministerium für Wirtschaft und Energie): Anwendungen für den Gesundheitssektor, 2015. http://www.trusted-cloud.de/239.php. Accessed February 5, 2015.

Boonstra, A.; Broekhuis, M.: Barriers to the Acceptance of Electronic Medical Records by Physicians from Systematic Review to Taxonomy and Interventions. Acta Informatica Medica 21 (2013), 2, pp. 129-134.

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

Buyya, R.; Yeo, C.S.; Venugopal, S.; Broberg, J.; Brandic, I.: Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems 25 (2009), 6, pp. 599–616.

Buyya, R.; Broberg, J.; Goscinsk, A. M.: Cloud Computing: Principles and Paradigms. John Wiley & Sons Inc., New Jersey, 2011.

Chang, H.H.; Chou, P.B.; Ramakrishnan, S.: An Ecosystem Approach for Healthcare Services Cloud. IEEE International Conference on e-Business Engineering, 2009.

Chai, S.; Bagchi-Sen, S.; Morrell, C.; Rao, H.R.; Upadhyaya, S.J.: Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. IEEE Transactions on Professional Communication 52 (2009), 2, pp. 167–182.

Chau, P.Y.K.; Hu, P.J.-H.: Information Technology Acceptance by Individual Professionals: A Model Comparison Approach. Decision Sciences 32 (2001), 4, pp. 699–719.

Chen, L.; Hoang, D.B.: Novel Data Protection Model in Healthcare Cloud. 13th IEEE International Conference on High Performance Computing and Communications (IEEE HPCC), 2011.

Chen, T.-S.; Liu, C.-H.; Chen, T.-L.; Chen, C.-S.; Bau, J.-G.; Lin, T.-C.: Secure Dynamic Access Control Scheme of PHR in Cloud Computing. Journal of Medical Systems 36 (2012a), 6, pp. 4005-4020.

Chen, Y.-Y.; Lu, J.-C.; Jan, J.-K.: A Secure EHR System Based on Hybrid Clouds. Journal of Medical Systems 36 (2012b), 5, pp. 3375-3384.

Chiang, W.-C.; Lin, H.-H.; Wu, T.-S.; Chen, C.-F.: Bulding a Cloud Service for Medical Image Processing Based on Service-Oriented Architecture. 4th International Conference on Biomedical Engineering and Informatics (BMEI), 2011.

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

Chow, R.; Golle, P.; Jakobsson, M.; Shi, E.; Staddon, J.; Masuoka, R.; Molina, J.: Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. ACM Workshop on Cloud Computing Security (CCSW), 2009.

Chowdhary, S.K.; Yadav, A.; Garg, N.: Cloud Computing: Future Prospect for e-Health. 3rd International Conference Electronics Computer Technology (ICECT), 2011.

Cooper, H.M.: Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews. Knowledge in Society 1 (1988), 1, pp. 104-126.

Cushman, R.; Froomkin, A.M.; Cava, A.; Abril, P.; Goodman, K.W.: Ethical, Legal and Social Issues for Personal Health Records and Applications. Journal of Biomedical Informatics 43 (2010), 5, pp. S51-S55.

Culnan, M.J.; Armstrong P.K.: Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 10 (1999), 1, pp. 104–115.

Common Criteria: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, 2012. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf. Accessed January 19, 2015.

Dalgaard, P.: Introductory Statistics with R. Springer, New York, 2002.

Duquenoy, P.; Mekawie, N.M.; Springett, M.: Patients, Trust and Ethics in Information Privacy in eHealth. In George, C.; Whitehouse, D.; Duquenoy, P. (Eds.): eHealth: Legal, Ethical and Governance Challenges, Springer, Berlin, 2012, pp. 275-295.

Davies, S.G.: Re-engineering the Right to Privacy: how Privacy has been transformed from a Right to a Commodity. In Agre, P.E.; Rotenberg, M. (Eds.): Technology and Privacy, MIT Press Cambridge, Massachusetts, 1997, pp. 143-165.

Davis, F.D.: Perceiver Usefulness, Perceived Ease of Use and User Acceptance of Information Technologie. MIS Quartely 13 (1989), 3, pp. 320.

Delgado, M.: The Evolution of Health Care IT: Are Current U.S. Privacy Policies Ready for the Clouds? 7th IEEE World Congress on Service (IEEE SERVICES), 2011.

Deng, M.; Petkovié, M.; Nalin, M.; Baroni, I.: A Home Healthcare System in the Cloud - Addressing Security and Privacy Challenges. 4th IEEE International Conference on Cloud Computing (IEEE CLOUD), 2011.

Deng, M.; Nalin, M.; Petkovié, M.; Baroni, I.; Marco, A.: Towards Trustworthy Health Platform Cloud. In Jonker, W.; Petković, M. (Eds.): Secure Data Management, Lecture Notes in Computer Science 7482, Berlin, 2012, pp 162-175.

DesRoches, C.M.; Campbell, E.G.; Rao, S.R.; Donelan, K.; Ferris, T.G.; Jha, A.; Kaushal, R; Levy, D.E.; Rosenbaum, S.; Shields, A.E.; Blumenthal, D.: Electronic Health Records in Ambulatory Care – A National Survey of Physicians. The New England Journal of Medicine 359 (2008), 1, pp. 50-60.

Dinev, T.; Hart, P.: Internet Privacy Concerns and their Antecedents - Measurement Validity and a Regression Model. Behaviour & Information Technology 23 (2004), 6, pp. 413-422.

Dinev, T.; Hu, Q.: The Centrality of Awareness in the Formation of User Behavioral Intention Toward Preventive Technologies in the Context of Voluntary Use. 4th Conference for Special Interest Group on Human-Computer Interaction (SIGHCI), 2005.

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

Dinev, T.; Hart, P.: Internet Privacy Concerns and Social Awareness as Determinants of Intention to transact. International Journal of E-Commerce 10 (2006b), 2, pp. 7-29.

Dinev, T.; Bellotto, M.; Hart, P.; Russo, V.; Serra, I.; Colautti, C.: Internet Users' Privacy Concerns and Beliefs about Government Surveillance: an Exploratory Study of Differences between Italy and the United States, Journal of Global Information Management 14 (2006a), 4, pp. 57–93.

Dinev, T.; Goo, J.; Hu, Q.; Nam, K.: User Behavior toward Preventive Technologies – Cultural Differences between the United States and South Korea. 14th European Conference of Information Systems (ECIS), 2006b.

Dinev, T.; Hu, Q.: The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information Systems 8 (2007), 7, pp. 386-408.

Dinev, T.: Internet Users' Beliefs about Government Surveillance – The Role of Social Awareness and Internet Literacy. 41st Hawaii International Conference on System Sciences (HICSS), 2008.

Dinev, T.; Goo, J.; Hu, Q.; Nam, K.: User Behavior toward Preventive Technologies – Cultural Differences between the United States and South Korea. Information Systems Journal 19 (2009), 4, pp. 391-412.

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

Dinev, T.; Xu, H.; Smith, H.J.; Hart, P.: Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. European Journal of Information Systems 22 (2013), 3, pp. 295-316.

Dünnebeil, S.; Sunyaev, A.; Blohm, I.; Leimeister, J.M.; Krcmar, H.: Determinants of Physicians' Technology Acceptance for e-Health in Ambulatory Care. International Journal of Medical Informatics 81 (2012), 11, pp. 746-760.

Eastlake, D.; Jones, P.: US Secure Hash Algorithm 1 (SHA1). RFC 3174, IETF, 2001.

Ekonomou, E.; Fan, L.; Buchanan, W.; Thüemmler, C.: An Integrated Cloud-Based Healthcare Infrastructure. 3rd IEEE International Conference on Coud Computing Technology and Science (IEEE CloudCom), 2011.

Ermakova, T.: Comparison of Secret-Sharing Schemes for Private Information Discovery. Master Thesis, Humboldt-University of Berlin, Germany, 2011.

Ermakova, T.; Fabian, B.: Secret Sharing for Health Data in Multi-Provider Clouds. 15th IEEE Conference on Business Informatics (IEEE CBI), 2013.

Ermakova, T.; Huenges, J.; Erek, K.; Zarnekow, R.: Cloud Computing in Healthcare – A Literature Review on Current State of Research. 19th Americas Conference on Information Systems (AMCIS), 2013a.

Ermakova, T.; Fabian, B.; Zarnekow, R.: Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios. 19th Americas Conference on Information Systems (AMCIS), 2013b.

Ermakova, T.; Preuße, S.; Weimann, P.; Zarnekow, R.: Reduzierung von Schwachstellen in Prozessen der Krankenhauseinrichtungen durch cloud-basierte Lösungen am Beispiel der Patientenversorgung. 43th Jahrestagung der Gesellschaft für Informatik (INFORMATIK), 2013c.

Ermakova, T.; Fabian, B.; Zarnekow, R.: Acceptance of Health Clouds – A Privacy Calculus Perspective. 22th European Conference on Information Systems (ECIS), 2014a.

Ermakova, T.; Baumann, A.; Fabian, B.; Krasnova, H.: Privacy Policies and Users' Trust: Does Readability Matter? 20th Americas Conference on Information Systems (AMCIS), 2014b.

Ermakova, T.; Fabian, B.; Babina, E.: Readability of Privacy Policies of Healthcare Websites. 12th International Conference on Wirtschaftsinformatik (WI), 2015a.

Ermakova, T.: Understanding Physicians' Adoption of Health Clouds. 4th International Conference on Information Technology Convergence and Services (ITCS), 2015.

Ermakova, T.; Fabian, B.; Zarnekow, R.: Improving Acceptance of Health Clouds. In Submission, 2015b.

European Parliament and Council: Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 on The Protection of Individuals with Regard to The Processing of Personal Data and on The Free Movement of Such Data. Official Journal 281 (1995), 31, pp. 0031 – 0050.

Fabian, B.; Gürses, S.; Heisel, M.; Santen, T.; Schmidt, H.: A Comparison of Security Requirements Engineering Methods. Requirements Engineering Journal 15 (2010), 1, pp. 7-40.

Fabian, B.; Ermakova, T.; Müller, C.: SHARDIS: A Privacy-Enhanced Discovery Service for RFID-Based Product Information. IEEE Transactions on Industrial Informatics 8 (2012), 3, pp. 707 – 718.

Fabian, B.; Ermakova, T.; Junghanns, P.: Collaborative and Secure Sharing of Healthcare Data in Multi-Clouds. Information Systems 48 (2014), pp. 132–150.

Fan, J.; Lv, J.: A Selective Overview of Variable Selection in High Dimensional Feature Space. Statistica Sinica 20 (2010), pp. 101–148.

Federal Statistical Office: Germany's Population by 2060: Results of the 12th Coordinated Population Projection, 2009. https://www.destatis.de/EN/Publications/Specialized/Population/GermanyPopulation2060.pdf?__blob=publicationFile. Accessed January 19, 2015.

Feldman, L.; Turow, J.; Meltzer, K.: Open to Exploitation: American Shoppers Online and Offline. Annenberg Public Policy Center, 2005. http://repository.upenn.edu/asc_papers/35. Accessed December 19, 2014.

Fernández-Cardeñosa, G.; de la Torre-Díez, I.; López-Coronado, M.; Rodrigues, J.J.P.C.: Analysis of Cloud-Based Solutions on EHRs Systems in Different Scenarios. Journal of Medical Systems 36 (2012), 6, pp. 3777-3782.

Ferraiolo, D.F.; Kuhn, D.R.; Chandramouli, R.: Role-Based Access Control. Artech House, Massachusetts, 2007.

Foster, I.; Zhao, Y.; Raicu, I.; Lu, S.: Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop (GCE), 2008.

Fox, J.; Weisberg, S.: An R Companion to Applied Regression, Second Edition. SAGE, 2011.

Geambasu, R.; Kohno, T.; Levy, A.A.; Levy, H.M.: Vanish: Increasing Data Privacy with Self-Destructing Data. 18th USENIX Security Symposium (USENIX Security), 2009.

Gefen, D.; Silver, M.: Lessons Learned from the Successful Adoption of an ERP System. 5th International Conference of the Decision Sciences Institute (IDSI), 1999.

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

Gefen, D.: E-Commerce: The Role of Familiarity and Trust. Omega 28 (2000), 6, pp. 725-737.

Gefen, D.: Customer Loyalty in E-Commerce. Journal of the Association for Information Systems 3 (2002), pp. 27-51.

Gefen, D.; Karahanna, E.; Straub, D.W.: Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly 27 (2003), 1, pp. 51-90.

Gefen, D.; Straub, D.: Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e-Services. Omega 32 (2004), pp. 407–424.

Gefen, D.; Rigdon, E.; Straub, D.: An Update and Extension to SEM Guidelines for Administrative and Social Science Research. MIS Quarterly 35 (2011), 2, pp. iii-xiv.

Graber, M.A.; D'Alessandro, D.M., Johnson-West, J.: Reading Level of Privacy Policies on Internet Health Web Sites. Journal of Family Practice 51 (2002), 7, pp. 642-642.

Gürses, S.; Jahnke, J.H.; Obry, C.; Onabajo, A.; Santen, T.; Price, M.: Eliciting Confidentiality Requirements in Practice. 15th Annual International Conference hosted by the IBM Centers for Advanced Studies (CASCON), 2005.

Gürses, S.; Berendt, B.; Santen, T.: Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments. Workshop on Ubiquitous Knowledge Discovery for Users at ECML/PKDD (UKDU), 2006.

Gürses, S.; Santen, T.: Contextualizing Security Goals: A Method for Multilateral Security Requirements Elicitation. Sicherheit 2006 - Schutz und Zuverlässigkeit, 2006.

Gürses, S.: Multilateral Privacy Requirements Analysis in Online Social Networks. PhD Thesis, K.U. Leuven, Belgium, 2010.

Guo, L.; Chen, F.; Chen, L.; Tang, X.: The Building of Cloud Computing Environment for E-Health. International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010.

Halbe, B.; Münzel, H.; Preusker, U.K.; Rau, F.: Krankenhausfinanzierungsreformgesetz (KHRG). Auswirkungen für Krankenhäuser. medhochzwei Verlag, Heidelberg, 2010.

Hann, I.-H.; Hui, K.-L.; Lee, S.-Y.T.; Png, I.P.L.: Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. Journal of Management Information Systems 24 (2007), 2, pp.13–42.

Hanner, N.; Ermakova, T.; Repschläger, J.; Zarnekow, R.: Designing a Business Model for a Cloud Marketplace for Healthcare. In Krcmar, H.; Reussner, R.; Rumpe, B. (Eds.): Trusted Cloud Computing, Springer, 2014.

Hardesty, L.: Big Medical Data, 2013. http://web.mit.edu/newsoffice/2013/big-medical-data-0125.html. Accessed December 22, 2014.

Haskew, J.; Rø, G.; Saito, K.; Turner, K.; Odhiambo, G.; Wamae, A.; Sharif, S.; Sugishita, T.: Implementation of a Cloud-Based Electronic Medical Record for Maternal and Child Health in Rural Kenya. International Journal of Medical Informatics 84 (2015), 5, pp. 349–354.

Hastie, T.; Tibshirani, R.; Friedman, J.: The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Second Edition. Springer Series in Statistics, 2009.

He, C.; Jin, X.; Zhao, Z.; Xiang, T.: A Cloud Computing Solution for Hospital Information System. 2nd IEEE International Conference on Intelligent Computing and Intelligent Systems (IEEE ICIS), 2010.

Hevner, A.R.; March, S.T.; Park, J.; Ram, S.: Design Science in Information Systems Research. MIS Quarterly 28 (2004), 1, pp. 75-105.

Hoang, D.B.; Chen, L.: Mobile Cloud for Assistive Healthcare (MoCAsH). 5th IEEE Asia-Pacific Services Computing Conference (IEEE APSCC), 2010.

Hong, W.; Thong, J.Y.L.: Internet Privacy Concerns: an Integrated Conceptualization and Four Empirical Studies". MIS Quarterly 37 (2013), 1, pp. 275-298.

Hoyert, D.L.; Xu, J.: Deaths: Preliminary Data for 2011 - Selected Causes. National Vital Statistics Reports 61 (2012), 6, pp. 40-42.

Huang, Q.; Ye, L.; Yu, M.; Wu, F.; Liang, R.: Medical Information Integration Based Cloud Computing. International Conference on Network Computing and Information Security (NCIS), 2011.

Huesch, M.D.: Privacy Threats when Seeking Online Health Information. JAMA Internal Medicine 173 (2013), 19, pp. 1838-1840.

Hui, K.L.; Teo, H.H.; Lee, S.Y.T.: The Value of Privacy Assurance: an Exploratory Field Experiment. MIS Quarterly 31 (2007), 1, pp. 19-33.

Hsu, P.-F.; Ray, S.; Li-Hsieh, Y.-Y.: Examining Cloud Computing Adoption Intention, Pricing Mechanism, and Deployment Model. International Journal of Information Management 34 (2014), 4, pp. 474–488.

Jensen, C.; Potts, C.; Jensen, C.: Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. International Journal of Human-Computer Studies 63 (2005), 1-2, pp. 203-227.

Ion, I.; Sachdeva, N.; Kumaraguru, P.; Capkun, S.: Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage. 7th Symposium on Usable Privacy and Security (SOUPS), 2011.

James, G.; Witten, D.; Hastie, T.; Tibshirani, R.: An Introduction to Statistical Learning with Applications in R. Springer Texts in Statistics, 2013.

Jarvenpaa, S.; Tractinsky, N.; Saarinen, L.; Vitale, M.: Consumer Trust in an Internet Store: a Crosscultural Validation. Journal of Computer-Mediated Communication 5 (1999), 2.

Jarvenpaa, S.; Tractinsky, N.; Vitale, M.: Consumer Trust in an Internet store. Information Technology and Management 1 (2000), 1–2, pp. 45–71.

Kaletsch, A.; Sunyaev, A.: Privacy Engineering: Personal Health Records in Cloud Computing Environments. International Conference on Information Systems (ICIS), 2011.

Kanagaraj, G.; Sumathi, A.C.: Proposal of an Open-Source Cloud Computing System for Exchanging Medical Images of a Hospital Information System. 3rd International Conference Trends in Information Sciences and Computing, 2011.

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

King, T.; Brankovic, L.; Gillard, P.: Perspectives of Australian Adults about Protecting the Privacy of Their Health Information in Statistical Databases. International Journal of Medical Informatics 81 (2012), 4, pp. 279-289.

Kochanek, K.D.; Xu, J.; Murphy, S.L.; Miniño, A.M.; Kung, H.-C.: Deaths: Final Data for 2009. National Vital Statistics Report 60 (2011), 3, pp. 1-116.

Kochhar, R.: 10 Projections for the Global Population in 2050. Pew Research Center, 2014. http://www.pewresearch.org/fact-tank/2014/02/03/10-projections-for-the-global-population-in-2050/. Accessed April 10, 2015.

Koufi, V.; Malamateniou, F.; Vassilacopoulos, G.: Ubiquitous Access to Cloud Emergency Medical Services. 10th IEEE International Conference Information Technology and Applications Biomedicine (IEEE ITAB), 2010.

Korzaan, M.L.; Boswell, K.T.: The Influence of Personality Traits and Information Privacy Concerns on Behavioral Intentions. Journal of Computer Information Systems 48 (2008), 4, pp. 15–24.

Krasnova, H.; Spiekermann, S.; Koroleva, K.; Hildebrandt, T.: Online Social Networks: Why We Disclose. Journal of Information Technology 25 (2009), 2, pp. 109–125.

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

Krawczyk, H.: Distributed Fingerprints and Secure Information Dispersal. 12th Annual ACM Symposium on Principles of Distributed Computing (PODC), 1993.

Krawczyk, H.: Secret Sharing Made Short. 13th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO), 1994.

Kunz, S.; Evdokimov, S.; Fabian, B.; Stieger, B.; Strembeck, M.: Role-Based Access Control for Information Federations in the Industrial Service Sector. 18th European Conference on Information Systems (ECIS), 2010.

Lafky, D.B.; Horan, T.A.: Personal Health Records: Consumer Attitudes toward Privacy and Security of their Personal Health Information. Health Informatics Journal 17 (2011), 1, pp. 63-71.

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

Laudon, K.C.; Laudon, J.P.; Schoder, D.: Wirtschaftsinformatik - Eine Einführung, 2. aktualisierte Auflage. Pearson Studium, 2010.

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

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

Li, Y.: Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework. Decision Support Systems 54 (2012), pp. 471-481.

Li, Y.: The Impact of Disposition to Privacy, Website Reputation and Website Familiarity on Information Privacy Concerns. Decision Support Systems 57 (2013), pp. 343-354.

Li, Y.; Baron, J.: Behavioral Research Data Analysis with R. Springer, New York, 2012.

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. 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm), 2010.

Li, Z.-R.; Chang, E.-C.; Huang, K.-H.; Lai, F.: A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform. 15th IEEE International Symposium on Consumer Electronics (IEEE ISCE), 2011a.

Li, M.; Yu, S.; Cao, N.; Lou, W.: Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing. 31st International Conference on Distributed Computing System (ICDCS), 2011b.

Li, H.; Sarathy, R.; Xu, H.: The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors. Decision Support Systems 51 (2011c), 3, pp. 434-445.

Li, F.; Zou, X.; Liu, P.; Chen J.Y.: New Threats to Health Data Privacy. BMC Bioinformatics 12 (2011d), 12, p. S7.

Li, Y.; Chang, K.-C.: A Study on User Acceptance of Cloud Computing: A Multi-Theoretical Perspective. Americas Conference on Information Systems (AMCIS), 2012.

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 (TPDS) 24 (2012), 1, pp. 131-143.

Lian, J.; Yen, D.C.; Wang, Y.: An Exploratory Study to Understand the Critical Factors Affecting the Decision to Adopt Cloud Computing in Taiwan Hospital. International Journal of Information Management 34 (2014), 1, pp. 28-36.

Liu, Y.; Wang, Y.; Jin, Y.: Research on the Improvement of MongoDB Auto-Sharding in Cloud Environment. 7th International Conference on Computer Science and Education (ICCSE), 2012.

Loehr, H.; Sadeghi, A.-R.; Winandy, M.: Securing the E-Health Cloud. 1st ACM International Health Informatics Symposium (IHI), 2010.

Lowry, R.: Concepts & Applications of Inferential Statistics, 2013. http://vassarstats.net/textbook/index.html. Accessed February 11, 2015.

Luo, W.; Najdawi, M.: Trust-Building Measures: a Review of Consumer Health Portals. Communications of the ACM 47 (2004), 1, pp. 109-113.

Lupse, O.S.; Stoicu-Tivadar, L.; Golie, C.: Assisted Prescription Based on Successful Treatments. 4th IEEE International Conference on e-Health and Bioengineering (IEEE EHB), 2013.

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

Malhotra, N.; Kim, S.; Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15 (2004), 4, pp. 336-355.

Mayer, R.C.; Davis, J.H.; Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management Review 20 (1995), 3, pp. 709–734.

Mani, G.; Li, W.: 3D Web Based Surgical Training Through Comparative Analysis. 18th International Conference on 3D Web (Web3D), 2013.

Manyika, J.; Chui, M.; Bughin, J.; Dobbs, R.; Bisson, P.; Marrs, A.: Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy. Technical Report, McKinsey Global Institute, 2013. http://www.mckinsey.com/insights/business_technology/disruptive_technologies. Accessed February 11, 2015.

Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A.: Cloud Computing – the Business Perspective. Decision Support Systems 51 (2011), 1, pp. 176–189.

McDonald, A.M.; Cranor L.F.: The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 4 (2008), 3, pp. 540-565.

McDonald, A.M.; Reeder, R.W., Kelley, P.G., Cranor, L.F.: A Comparative Study of Online Privacy Policies and Formats. Privacy Enhancing Technologies 5672 (2009), pp. 37-55.

McGraw, D.; Dempsey, J.X.; Harris, L.; Goldman, J.: Privacy as an Enabler, not an Impediment: Building Trust into Health Information Exchange. Health Affairs 28 (2009), 2, pp. 416-427.

McKnight, D.H.; Cummings, L.L.; Chervany, N.L.: Initial Trust Formation in New Organizational Relationships. Academy of Management Review 23 (1998), 3, pp. 472-490.

McKnight, D.H.; Choudhury, V.; Kacmar, C.: Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. Information Systems Research 13 (2002), 3, pp. 334-359.

Mell, P.; Grace, T.: The NIST Definition of Cloud Computing. Special Publication 800-145, National Institute of Standards and Technology (NIST), 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed February 11, 2015.

Mills, B.N.; Znati, T.: Increasing DHT Data Security by Scattering Data. 17th International Conference on Computer Communications and Networks (ICCCN), 2008.

Milne, G.R.; Rohm, A.: Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives. Journal of Public Policy and Marketing 19 (2000), 2, pp. 238-249.

Milne, G.R.; Culnan, M.J.: Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't Read) Privacy Notices. Journal of Interactive Marketing 18 (2004), 3, pp. 15-29.

Mohammed, S.; Fiaidhi, J.: The Roadmap for Sharing Electronic Health Records: The Emerging Ubiquity and Cloud Computing Trends. 2nd International Conference on Future Generation Information Technology (FGIT), 2010.

Moores, T.T.: Towards an Integrated Model of IT Acceptance in Healthcare. Decision Support Systems 53 (2012), 3, pp. 507-516.

Myung, I.: The Importance of Complexity in Model Selection. Journal of Mathematical Psychology 44 (2000), pp. 190-204.

Najaftorkaman, M.; Ghapanchi, A.H.: Antecedents to the User Adoption of Electronic Medical Record. 18th Pacific Asia Conference on Information Systems (PACIS), 2014.

Nass, S.J.; Levit, L.A.; Gostin, L.O.: Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. National Academies Press, Washington, 2009.

Nordin, M.I.; Hassan, M.I.: Cloud Resource Broker in the Optimization of Medical Image Retrieval System: A Proposed Goal-Based Request in Medical Application. National Postgraduate Conference (NPC), 2011.

Nordin, M.I.; Abdullah, A.; Hassan, M.I.: Goal-Based Request Cloud Resource Broker in Medical Application. International Conference on Telecommunication Technology and Applications (CSIT), 2011.

Nordin, M.I.; Amin, A.H.M.; Shah, S.N.M.: Agent Based Resource Broker for Medical Informatics Application in Clouds. International Conference on Computer & Information Science (ICCIS), 2012.

Nematzadeh, A.; Camp, L.J.: Threat Analysis of Online Health Information System. 3rd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA), 2010.

Opitz, N.; Langkau, T.F.; Schmidt, N.H.; Kolbe, L.M.: Technology Acceptance of Cloud Computing: Empirical Evidence from German IT Departments. 45th Hawaii International Conference on System Sciences (HICSS), 2012.

Osterhaus, L.C.: Cloud Computing and Health Information. B Sides (2010).

OASIS (Advancing Open Standards for the Information Society): Web Services Security v1.1.1. https://www.oasis-open.org/standards#wssv1.1.1. Accessed February 11, 2015.

OMG (Object Management Group): Business Process Model and Notation. http://www.bpmn.org/. Accessed February 11, 2015.

Pavlou, P.; H. Liang; Xue, Y.: Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principle–Agent Perspective? MIS Quarterly 31 (2007), 1, pp. 105–136.

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

Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems 24 (2008), 3, pp. 45-77.

Petcu, D.: Multi-Cloud: Expectations and Current Approaches. International Workshop on Multi-Cloud Applications and Federated Clouds (MultiCloud), 2013.

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

Peterson, D.; Meinert, D.; Criswell II, J.; Crossland, M.: Consumer Trust: Privacy Policies and Third-Party Seals. Journal of Small Business and Enterprise Development 14 (2007), 4, pp. 654-669.

Perera, G.; Holbrook, A.; Thabane, L.; Foster, G.; Willison, D.J.: Views on Health Information Sharing and Privacy from Primary Care Practices Using Electronic Medical Records. International Journal of Medical Informatics 80 (2011), 2, pp. 94-101.

Poulymenopoulou, M.; Malamateniou, F.; Vassilacopoulos, G.: E-EPR: a Cloud-Based Architecture of an Electronic Emergency Patient Record. 4th International Conference on PErvasive Technologies Related to Assistive Environments (PETRA), 2011.

Pollach, I.: What's Wrong with Online Privacy Policies? Communications of the ACM 50 (2007), 9, pp. 103-108.

R Development Core Team: R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria, 2012. http://www.R-project.org/. Accessed February 11, 2015.

Rabin, M.: Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. Journal of the ACM 36 (1989), pp. 335-348.

Ratnam, K.A.; Dominic, D.D.: Cloud Services - Enhancing the Malaysian Healthcare Sector. International Conference on Computer & Information Science (ICCIS), 2012.

Rauer, U.: Patient Trust in Internet-based Health Records: An Analysis Across Operator Types and Levels of Patient Involvement in Germany. Policy & Internet 4 (2012), 2, pp. 1-42.

Richards, R.J.: A Study of the Intent to Fully Utilize Electronic Personal Health Records in the Context of Privacy and Trust. PhD Thesis, University of North Texas, USA, 2012. http://digital.library.unt.edu/ark:/67531/metadc115145/m2/1/high_res_d/dissertation.pdf. Accessed February 11, 2015.

Ringle, C.M.; Wende, S.; Will, S.: SmartPLS 2.0 (M3) Beta, Hamburg, Germany. http://www.smartpls.de. Accessed February 11, 2015.

Riordan, F.; Papoutsi, C.; Reed, J.E.; Marston, C.; Bell, D.; Majeed, A.: Patient and Public Attitudes Towards Informed Consent Models and Levels of Awareness of Electronic Health Records in the UK. International Journal of Medical Informatics 84 (2015), 4, pp. 237–247.

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

Rolim, C.O.; Koch, F.L.; Westphall, C.B.; Werner, J.; Fracalossi, A.; Salvador, G.S.: A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions. 2nd International Conference on eHealth, Telemedicine and Social Medicine (ETELEMED), 2010.

Rodrigues, R.; Liskov, B.: High Availability in DHTs: Erasure Coding vs. Replication. 4th International Workshop on Peer-to-Peer Systems (IPTPS), 2005.

Rupp, C.: UML 2 glasklar: Praxiswissen für die UML-Modellierung und –Zertifizierung. Carl Hanser Verlag, 2005.

Shamir, A.: How to Share a Secret. Communications of the ACM 22 (1979), 11, pp. 612-613.

Sharieh, S.; Franek, F.; Ferworn, A.: Using Cloud Computing for Medical Appications. 15th Communications and Networking Simulation Symposium (CNS), 2012.

Sharma, P.N.; Kim, K.H.: Model Selection in Information Systems Research Using Partial Least Squares Based Structural Equation Modeling. 33rd International Conference on Information Systems (ICIS), 2012.

Sheskin, D.J.: Handbook of Parametric and Nonparametric Statistical Procedures, 3rd Edition. CRC Press, 2004.

Shim, S.S.Y.; Bhalla, G.; Pendyala, V.: Federated Identity Management. IEEE Computer 38 (2005), 12, pp. 120-122.

Shini, S.G; Thomas, T.; Chithraranjan, K.: Cloud-Based Medical Image Exchange Security Challenges. Procedia Engineering 38 (2012), pp. 3454–3461.

Simon, S.R.; Kalshal, R.; Cleary, P.D.; Jenter, C.A.; Volk, L.A.; Oray, E.J.; Burdick E.; Poon, E.G.; Batees, W.W.: Physicians and Electronic Health Records: A Statewide Survey. Archives of Internal Medicine 167 (2007), 5, pp. 507-512.

Simon, S.R.; Evans, J.S.; Benjamin, A.; Delano, D.; Bates, D.W.: Patients' Attitudes toward Electronic Health Information Exchange: Qualitative Study. Journal of Medical Internet Research 11 (2009), 3, p. e30.

Slawik, M.; Zickau, S.; Thatmann, T.; Repschläger, J.; Ermakova, T.; Küpper, A.; Zarnekow, R.: Innovative Architektur für sicheres Cloud Computing: Beispiel eines Cloud-Ecosystems im Gesundheitswesen. 42th Jahrestagung der Gesellschaft für Informatik (INFORMATIK), 2012.

Slawik, M.; Ermakova, T.; Repschläger, J.; Küpper, A.; Zarnekow, R.: Securing Medical SaaS Solutions Using a Novel End-to-End Encryption Protocol. 22th European Conference on Information Systems (ECIS), 2014.

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

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

Son, J.Y.; Kim, S.S.: Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS Quarterly 32 (2008), 3, pp. 503–529.

Stallings, W.: Cryptography and Network Security: Principles and Practice. Prentice Hall, 2010.

Statistisches Bundesamt: Statistisches Bundesamt. www.destatis.de. Accessed February 12, 2015.

Streiner, D.L.; Norman, G.R.: Correction for Multiple Testing: Is there a Resolution? Chest 140 (2011), 1, pp. 16–18.

Stinson, D.R.: An Explication of Secret Sharing Schemes. Des. Codes Cryptography 2 (1992), 4, pp. 357-390.

Sultan, F.; Urban, G.L.; Shankar, V.; Bart, I.Y.: Determinants and Role of Trust in e-Business: A Large Scale Empirical Study. Working Paper 4282-02, MIT Sloan School of Management, USA, 2002. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=380404. Accessed February 9, 2015.

Sultan, N.: Making Use of Cloud Computing for Healthcare Provision: Opportunities and Challenges. International Journal of Information Management 34 (2014a), 2, pp. 177–184.

Sultan, N.: Discovering the Potential of Cloud Computing in Accelerating the Search for Curing Serious Illnesses. International Journal of Information Management 34 (2014b), 2, pp. 221–225.

Sunyaev, A.; Dehling, T.; Taylor, P.L.; Mandl, K.D.: Availability and Quality of Mobile Health App Privacy Policies. Journal of the American Medical Informatics Association (2014).

Tak, B.C.; Urgaonkar, B.; Sivasubramaniam, A.: To Move or Not to Move: The Economics of Cloud Computing. 3rd USENIX Workshop on Hot Topics in Cloud Computing (USENIX HotCloud), 2011.

TAPAS (Technology Assisted Practice Application Suite): TAPAS Security Requirements, 2004. http://www.opentapas.org/docs/security_requ.html. Accessed December 19, 2014.

Teixeira, P.A.; Gordon, P.; Camhi, E.; Bakken, S.: HIV Patients' Willingness to Share Personal Health Information Electronically. Patient Education and Counseling 84 (2011), 2, pp. e9-e12.

Thomas, R.; Sandhu, R.: Task-Based Authorization Controls (TBAC). IFIP WG11.3 Conference on Database Security, 1997.

TRESOR: TRESOR. http://www.cloud-tresor.com/. Accessed February 8, 2015.

TRUSTe: TRUSTe. http://www.truste.com/. Accessed February 8, 2015.

Tsai, J.Y.; Egelman, S.; Cranor, L.; Acquisti, A.: The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research 22 (2011), 2, pp. 254-268.

TNS Emnid: Klassische Medien punkten in der Informationsgesellschaft 2.0—noch!, 2009. http://www.tns-emnid.com/presse/presseinformation.asp?prID=837. Accessed February 8, 2015.

U.S. Department of Health and Human Services: Health Information Privacy. http://www.hhs.gov/ocr/privacy/. Accessed February 8, 2015.

Undem, T.: Consumers and Health Information Technology: A National Survey, 2010. http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/C/PDF%20ConsumersHealthInfoTechnologyNationalSurvey.pdf. Accessed February 8, 2015.

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

Vathanophas, V.; Pacharapha, T.: Information Technology Acceptance in Healthcare Service: The Study of Electronic Medical Record (EMR) in Thailand. Conference on Technology Management for Global Economic Growth (PICMET), 2010.

Vazhenin, D.: Cloud-Based Web-Service for Health 2.0. Joint International Conference on Human-Centered Computer Environments (HCCE), 2012.

Venkatesh, V.; Davis, F.D.: A Theoretical Extension of the Technology. Management Science 46 (2000), 2, pp. 186 –204.

Venkatesh, V.; Bala, H.: Technology Acceptance Model 3. Decision Sciences 39 (2008), 2, pp. 273-315.

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

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

VHB (Verband der Hochschullehrer für Betriebswirtschaft e.V.): VHB Jourqual 2.1, 2011. http://vhbonline.org/service/jourqual/vhb-jourqual-21-2011/jq21neu/. Accessed February 11, 2015.

Verizon: 2014 Data Breach Investigations Report, 2014. http://www.verizonenterprise.com/DBIR/2013/. Accessed February 8, 2015.

vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. 17th European Conference on Information Systems (ECIS), 2009.

Wang, X.; Tan, Y.: Application of Cloud Computing in the Health Information System. International Conference on Computer Application and System Modeling (ICCASM), 2010.

Warren, S.D.; Brandeis, D.L.: The Right to Privacy. Harvard Law Review 4 (1890), 5, pp. 193–220.

Webster, J.; Watson, R.T.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 26 (2002), 2, pp. xiii-xxiii.

Westin, A. F.: Privacy and Freedom. Atheneum Publishers, New York, 1967.

Whiddett, R.; Hunter, I.; Engelbrecht, J.; Handy, J.: Patients' Attitudes towards Sharing Their Health Information. International Journal of Medical Informatics 75 (2006), 7, pp. 530-541.

Wilde, T.; Hess, T.: Forschungsmethoden der Wirtschaftsinformatik. Wirtschaftsinformatik (WI) 49 (2007), 4, pp. 280–287.

Winter, A.; Ammenwerth, E.; Brigl, B.; Haux, R.: Grundlagen von Informations- und Kommunikationstechnologien im Krankenhaus. In Herbig, B.; Büssing, A. (Eds.): Informations- und Kommunikationstechnologien im Krankenhaus: Grundlagen, Umsetzung, Chancen und Risiken, Schattauer, pp. 7-28.

Whitman, M.E.; Mattord, H.J.: Management of Information Security. Cengage Learning, 2013.

WKWI (Wissenschaftliche Kommission Wirtschaftsinformatik im Verband der Hochschullehrer für Betriebswirtschaftslehre): WI-Orientierungslisten: WI-Journalliste 2008 sowie WI- Liste der Konferenzen, Proceedings und Lecture Notes 2008, 2008. http://gcc.uni-paderborn.de/www/WI/WI2/wi2_lit.nsf/0/549991b84925b9d5c12573d200360077/$FILE/Orientierungslisten_WKWI_GIFB5_ds41.pdf. Accessed February 11, 2015.

Wu, C.-S.; Khoury, I.: E-Healthcare Web Service Broker Infrastructure in Cloud Environment. 8th IEEE World Congress on Services (IEEE SERVICES), 2012.

Wu, R.; Ahn, G.-J.; Hu, H.: Secure Sharing of Electronic Health Records in Clouds. 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012.

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

Xu, H.: The Effects of Self-Construal and Perceived Control on Privacy Concerns. 29th International Conference on Information Systems (ICIS), 2007.

Xu, H.; Dinev, T.; Smith, H.J.; Hart, P.: Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. 29th International Conference on Information Systems (ICIS), 2008.

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

Xu, H.; Teo, H.H.; Tan, B.C.Y.; Agarwal, R.: Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research 23 (2012), 4, pp. 1342-1363.

Yao, M.Z.; Rice, R.E.; Wallis, K.: Predicting User Concerns about Online privacy. Journal of the American Society for Information Science and Technology 58 (2007), 5, pp. 710–722.

Yang, H.; Tate, M.: A Descriptive Literature Review and Classification of Cloud Computing Research. Communications of the Association for Information Systems 31 (2012), pp. 35-60.

Yu, S.; Wang, C.; Ren, K.; Wenjing L.: Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing. 29th Conference on Information Communications, 2010.

Zhang, R.; Liu, L.: Security Models and Requirements for Healthcare Application Clouds. 3rd IEEE International Conference on Cloud Computing (IEEE CLOUD), 2010.

Zhang, J.; Lu, J.: The District Medical Data Center Based on Cloud Computing. 5th International Conference on Computer Science & Education (ICCSE), 2010.

Zheng, Z.; Pavlou, P.: Toward a Causal Interpretation from Observational Data: A New Bayesian Networks Method for Structural Models with Latent Variables. Information Systems Research 21 (2010), 2, pp. 365-391.

Zickau, S.; Thatmann, D.; Ermakova, T.; Repschläger, J.; Zarnekow, R.; Küpper, A.: Enabling Location-Based Policies in a Healthcare Cloud Computing Environment. 3rd IEEE International Conference on Cloud Networking (IEEE CloudNet), 2014.

Zimmer, J.C.; Arsal, R.; Al-Marzouq, M.; Moore, D.; Grover, V.: Knowing your Customers: Using a Reciprocal Relationship to Enhance Voluntary Information Disclosure. Decision Support Systems 48 (2010), 2, pp. 395–406.

Zulman, D.M.; Nazi, K.M.; Turvey, C.L.; Wagner, T.H.; Woods, S.S.; An, L.C.: Patient Interest in Sharing Personal Health Record Information. Annals of Internal Medicine 155 (2011), 12, pp. 805-811.

11. Appendix

11.1 Introduction

Nr.	Publication	Ranking	
		WKWI, 2011	**VHB, 2011**
1	**Ermakova, T.**; Fabian, B.; Zarnekow, R.: Improving Acceptance of Health Clouds. In Submission, 2015b.		
2	**Ermakova, T.**: Understanding Physicians' Adoption of Health Clouds. 4th International Conference on Information Technology Convergence and Services (ITCS), 2015.		
3	**Ermakova, T.**; Fabian, B.; Babina, E.: Readability of Privacy Policies of Healthcare Websites. 12th International Conference on Wirtschaftsinformatik (WI), 2015a.	A	B
4	Fabian, B.; **Ermakova, T.**; Junghanns, P.: Collaborative and Secure Sharing of Healthcare Data in Multi-Clouds. Information Systems 48 (2014), pp. 132–150.	A	C
5	**Ermakova, T.**; Fabian, B.; Zarnekow, R.: Acceptance of Health Clouds – A Privacy Calculus Perspective. 22th European Conference on Information Systems (ECIS), 2014a.	A	B
6	**Ermakova, T.**; Baumann, A.; Fabian, B.; Krasnova, H.: Privacy Policies and Users' Trust: Does Readability Matter? 20th Americas Conference on Information Systems (AMCIS), 2014b.	B	D
7	Slawik, M.; **Ermakova, T.**; Repschläger, J.; Küpper, A.; Zarnekow, R.: Securing Medical SaaS Solutions Using a Novel End-to-End Encryption Protocol. 22th European Conference on Information Systems (ECIS), 2014.	A	B
8	Hanner, N.; **Ermakova, T.**; Repschläger, J.; Zarnekow, R.: Designing a Business Model for a Cloud Marketplace for Healthcare. Trusted Cloud Computing, Springer, 2014.		
9	Zickau, S.; Thatmann, D.; **Ermakova, T.**; Repschläger, J.; Zarnekow, R.; Küpper, A.: Enabling Location-Based Policies in a Healthcare Cloud Computing Environment. 3rd IEEE International Conference on Cloud Networking (IEEE CloudNet), 2014.		
10	**Ermakova, T.**; Fabian, B.: Secret Sharing for Health Data in Multi-Provider Clouds. 15th IEEE Conference on Business Informatics (IEEE CBI), 2013.		
11	**Ermakova, T.**; Huenges, J.; Erek, K.; Zarnekow, R.: Cloud Computing in Healthcare – A Literature Review on Current State of Research. 19th Americas Conference on Information Systems (AMCIS), 2013a.	B	D
12	**Ermakova, T.**; Preuße, S.; Weimann, P.; Zarnekow, R.: Reduzierung von Schwachstellen in Prozessen der Krankenhauseinrichtungen durch cloud-basierte Lösungen am Beispiel der Patientenversorgung. 43th Jahrestagung der Gesellschaft für Informatik (INFORMATIK), 2013c.	C	C

13	**Ermakova, T.**; Fabian, B.; Zarnekow, R.: Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios. 19th Americas Conference on Information Systems (AMCIS), 2013b.	B	D
14	Fabian, B.; **Ermakova, T.**; Müller, C.: SHARDIS: A Privacy-Enhanced Discovery Service for RFID-Based Product Information. IEEE Transactions on Industrial Informatics 8 (2012), 3, pp. 707–718.	A	
15	Slawik, M.; Zickau, S.; Thatmann, T.; Repschläger, J.; **Ermakova, T.**; Küpper, A.; Zarnekow, R.: Innovative Architektur für sicheres Cloud Computing: Beispiel eines Cloud-Ecosystems im Gesundheitswesen. 42th Jahrestagung der Gesellschaft für Informatik (INFORMATIK), 2012.	C	C

Table 28. Complete List of Publications

11.2 Investigating Acceptance of Health Clouds

Faktor	**Frage**
Verhaltensabsicht (Intention), Cloud Computing im Gesundheitswesen zu akzeptieren	Stellen Sie sich bitte vor: **Ihre sensiblen Patientendaten** können **verschlüsselt über ein cloud-basiertes System** aus Ihrer aktuellen an die weiterbehandelnde medizinische Einrichtung (z.B. Krankenhaus oder Arztpraxis) **zum richtigen Zeitpunkt** übermittelt werden. Inwieweit wären Sie bereit, unter den oben beschriebenen Voraussetzungen der Übermittlung Ihrer Patientendaten zuzustimmen, wenn ... ... Ihre Patientendaten **sonst nicht rechtzeitig** beim Empfänger ankommen könnten. ... es sich um einen **Notfall** handelt. ... Ihre Patientendaten **sonst per Fax** übermittelt werden könnten. ... Ihre Patientendaten **sonst per Taxi** übermittelt werden könnten. ... **Sie sich selber darum kümmern** müssten. ... **der aus Ihrer Sicht sensible Teil** Ihrer Patientendaten **nicht mit übermittelt** wird. ... Ihre Patientendaten **vor der Verschlüsselung pseudonymisiert** (unter Verwendung eines Pseudonyms anstatt von Ihren personenidentifizierenden Daten) werden. Antwortmöglichkeiten: 1: Gar nicht bereit. 2: Weitgehend nicht bereit. 3: Eher nicht bereit. 4: Weder noch. 5: Eher bereit. 6: Weitgehend bereit. 7: Vollständig bereit.
Wahrgenommene Vorteile des Cloud-Anwendungsszenarios	Inwieweit treffen die folgenden Aussagen auf Sie zu? Ich finde, dass **die Vorteile** des oben beschriebenen Anwendungsszenarios **überwiegen und meine Bedenken** bezüglich der möglichen Risiken **aufheben**. **Je größer die Vorteile** des oben beschriebenen Anwendungsszenarios sind, **desto mehr** tendiere ich dazu, **meine Bedenken** bezüglich der möglichen Risiken zu **ignorieren**. Im Großen und Ganzen sehe ich **mein Bedürfnis** nach dem oben beschriebenen Anwendungsszenario **größer, als meine Bedenken** bezüglich der möglichen Risiken.

	Antwortmöglichkeiten: 1: Trifft gar nicht zu. 2: Trifft weitgehend nicht zu. 3: Trifft eher nicht zu. 4: Weder noch. 5: Trifft eher zu. 6: Trifft weitgehend zu. 7: Trifft voll zu.
Bedenken über Privatsphäre – Nichtberichtigter Zugriff auf Patientendaten	Inwieweit wären Sie besorgt, dass … … **Nichtberechtigte Zugriffe** auf Ihre Patientendaten in der Cloud **haben können**. … Ihre Patientendaten in der Cloud **nicht genügend gegen den Zugriff durch Nichtberechtigte geschützt** sind. … der **Zugriff** auf Ihre Patientendaten in der Cloud **durch Nichtberechtigte kaum verhindert** werden kann. … der **Zugriff** auf Ihre Patientendaten in der Cloud **durch Nichtberechtigte kaum erkannt** werden kann. Antwortmöglichkeiten: 1: Gar nicht besorgt. 2: Nicht besorgt. 3: Eher nicht besorgt. 4: Weder noch. 5: Eher besorgt. 6: Besorgt. 7: Sehr besorgt.
Bedenken über Privatsphäre – Fehler in Patientendaten	Inwieweit wären Sie besorgt, dass … … **Nichtberechtigte** Ihre Patientendaten in der Cloud **unerwünscht modifizieren können**. … Ihre Patientendaten in der Cloud **nicht genügend gegen unerwünschte Modifikationen durch Nichtberechtigte geschützt** sind. … **unerwünschte Modifikationen** an Ihren Patientendaten in der Cloud **durch Nichtberechtigte kaum verhindert** werden können. … **unerwünschte Modifikationen** an Ihren Patientendaten in der Cloud **durch Nichtberechtigte kaum erkannt** werden können. … Ihre Patientendaten in der Cloud **nicht inhaltlich korrekt beim Empfänger ankommen können**. … Ihre Patientendaten in der Cloud **nicht zeitlich korrekt beim Empfänger ankommen können**. Antwortmöglichkeiten: 1: Gar nicht besorgt. 2: Nicht besorgt. 3: Eher nicht besorgt. 4: Weder noch. 5: Eher besorgt. 6: Besorgt. 7: Sehr besorgt.
Bedenken über Privatsphäre – Sammlung von Patientendaten	Inwieweit wären Sie besorgt, dass Ihre Patientendaten in der Cloud nach Abruf durch die weiterbehandelnde medizinische Einrichtung … … in der Cloud **nicht gelöscht** werden. … als Kopien in der Cloud **weiterhin erhalten bleiben**. … vom Cloud-Anbieter **gesammelt werden**. Antwortmöglichkeiten: 1: Gar nicht besorgt. 2: Nicht besorgt. 3: Eher nicht besorgt. 4: Weder noch. 5: Eher besorgt. 6: Besorgt. 7: Sehr besorgt.
Bedenken über Privatsphäre - Unberechtigte Nutzung von Patientendaten	Inwieweit wären Sie besorgt, dass **Ihre Patientendaten in der Cloud** … … von irgendjemandem **gefunden** werden können. … von irgendjemandem **manipuliert** werden können. … von irgendjemandem in einer Weise **genutzt** werden können, die Sie **nicht voraussehen** konnten. … von irgendjemandem **missbraucht** werden können. ... für Unternehmen oder unbekannte Dritte **ohne Ihr Wissen zugänglich gemacht** werden können. … an Unternehmen oder unbekannte Dritte **verkauft** werden können.

	… **gewerblich genutzt** werden können. … **ausgespäht** werden können. Antwortmöglichkeiten: 1: Gar nicht besorgt. 2: Nicht besorgt. 3: Eher nicht besorgt. 4: Weder noch. 5: Eher besorgt. 6: Besorgt. 7: Sehr besorgt.
Vertrauen in Regulierungsmechanismen	Inwieweit meinen Sie, dass **die momentanen gesetzlichen Regelungen**… … Ihre Patientendaten in der Cloud **wirksam vor Missbrauch schützen**. … **zuverlässig regeln**, wie Ihre Patientendaten in der Cloud **geschützt, gesammelt und verteilt** werden. … **ausreichend** sind, **dem Missbrauch** Ihrer Patientendaten in der Cloud **entgegenzuwirken**. Antwortmöglichkeiten: 1: Trifft gar nicht zu. 2: Trifft weitgehend nicht zu. 3: Trifft eher nicht zu. 4: Weder noch. 5: Trifft eher zu. 6: Trifft weitgehend zu. 7: Trifft voll zu.
Vertrauen in technologische Mechanismen	Inwieweit meinen Sie, dass **die momentanen technologischen Mechanismen** … … **wirksam vor Zugriffen und unerwünschten Modifikationen** an Ihren Patientendaten in der Cloud **durch Unberechtigte schützen** können. … **zuverlässig umsetzen** können, wie Ihre Patientendaten in der Cloud **geschützt, gesammelt und verteilt** werden. … **ausreichend** sein können, **den Zugriffen und unerwünschten Modifikationen** an Ihren Patientendaten in der Cloud **durch Unberechtigte entgegenzuwirken**. Antwortmöglichkeiten: 1: Trifft gar nicht zu. 2: Trifft weitgehend nicht zu. 3: Trifft eher nicht zu. 4: Weder noch. 5: Trifft eher zu. 6: Trifft weitgehend zu. 7: Trifft voll zu.
Vertrauen in Cloud-Anbieter (im Gesundheitswesen)	Inwieweit meinen Sie, dass **die Content- und Online-Speicherplatz-Anbieter**, die **im Gesundheitswesen** tätig sind, … … **zuverlässig umsetzen** können, wie Ihre Patientendaten in der Cloud **geschützt, gesammelt und verteilt** werden. … **vertrauenswürdig** sind. … **nach bestem Gewissen** handeln. Antwortmöglichkeiten: 1: Trifft gar nicht zu. 2: Trifft weitgehend nicht zu. 3: Trifft eher nicht zu. 4: Weder noch. 5: Trifft eher zu. 6: Trifft weitgehend zu. 7: Trifft voll zu.
Angegebener Wissenstand bzgl. Privatsphäre im Internet	Inwieweit treffen die folgenden Aussagen auf Sie zu? Ich **bin mir der Risiken und Schutzmechanismen** in Bezug auf meine Privatsphäre im Internet **bewusst**. Ich **verfolge die Nachrichten um die Risiken und Schutzverfahren** in Bezug auf meine Privatsphäre im Internet. Ich **informiere mich über Risiken** bezüglich meiner Privatsphäre im Internet und mögliche **Lösungen**, die man anwendet, um diese zu schützen. Antwortmöglichkeiten: 1: Trifft gar nicht zu. 2: Trifft weitgehend nicht zu. 3: Trifft eher nicht zu. 4: Weder noch. 5: Trifft eher zu. 6: Trifft weitgehend zu. 7: Trifft voll zu.
Geschlecht	Dürfen wir über Ihr Geschlecht fragen? Weiblich. Männlich.

Alter	Dürfen wir fragen, wie alt Sie ungefähr sind? Bitte wählen Sie eine der folgenden Antworten: < oder gleich 20 Jahre. 21 – 30 Jahre. 31 – 40 Jahre. 41 – 50 Jahre. 51 – 60 Jahre. 61 – 70 Jahre. > 70 Jahre. Ich möchte zu meinem Alter keine Auskunft geben.
Gesundheitszustand	Wie schätzen Sie Ihren momentanen Gesundheitszustand generell ein? Bitte wählen Sie eine der folgenden Antworten: Sehr gut. Gut. Eher gut. Weder gut, noch schlecht. Eher schlecht. Schlecht. Sehr schlecht.
Tatsächlicher Wissenstand bzgl. Privatsphäre im Internet	Kann Ihr E-Mail-Anbieter die von Ihnen an eine E-Mail angehängten Dokumente sehen und ändern? Bitte wählen Sie eine der folgenden Antworten: a) Er kann sie **weder** einsehen **noch** ändern. b) Er kann sie **sehen, aber nicht ändern**. c) Er kann sie **ggf. sowohl** sehen **als auch** ändern. d) Ich weiß es nicht. (Lösung: c) Was passiert Ihrer Meinung nach, wenn Sie eine bei einer E-Mail angehängte Datei von Ihrem E-Mail-Anbieter löschen? Bitte wählen Sie eine der folgenden Antworten: a) Die Datei wird, wie auf dem eigenen Computer, **permanent gelöscht**. b) Möglicherweise werden **Kopien für einige Wochen oder länger behalten**, bis das Unternehmen es schafft, sie alle zu löschen. c) Ich weiß es nicht. (Lösung: b) Welches der folgenden Protokolle stellt eine vertrauenswürdige E-Mail-Übertragung von Sender zu Empfänger sicher? Bitte wählen Sie einen oder mehrere Punkte aus der Liste aus. a) Sec4Mail-Verschlüsselung. b) POPSEC-Verschlüsselung. c) PGP-Verschlüsselung. d) SIMAP-Verschlüsselung. e) Ich weiß es nicht. (Lösung: c) Wie kann eine Webseite ihre Besucher voneinander unterscheiden? Bitte wählen Sie einen oder mehrere Punkte aus der Liste aus. a) Benutzername. b) IP-Adresse. c) Cookies. d) Die Version des Internetbrowsers und Einstellungen. e) Ich weiß es nicht. (Lösung: a, b, c, d) Welche der folgenden Aussagen ist richtig? Bitte wählen Sie einen oder mehrere Punkte aus der Liste aus. a) Wenn Sie im Internet **ohne Verschlüsselung** surfen, dann kann Ihr **Internetanbieter** den Inhalt der Webseiten, die Sie besuchen, beobachten. b) Wenn Sie im Internet **mit Verschlüsselung** surfen, dann kann Ihr **Internetanbieter** den Inhalt der Webseiten, die Sie besuchen, beobachten. c) Wenn Sie im Internet **mit Verschlüsselung** surfen, dann kann der **Webserver** den Inhalt der Webseiten, die Sie besuchen, beobachten. d) Wenn Sie im Internet **ohne Verschlüsselung** surfen, dann kann **jeder Router** auf dem Weg zum Webserver die Webseiten, die Sie besuchen, beobachten. e) Ich weiß es nicht. (Lösung: a, c, d) Welches der folgenden Protokolle wird zum Surfen im Internet genutzt? Bitte wählen Sie einen oder mehrere Punkte aus der Liste aus. a) HTTP. b) IMAP. c) TCP. d) IP. e) Ich weiß es nicht. (Lösung: a, c, d) Welche der folgenden Maßnahmen können Ihre Privatsphäre beim Surfen im Internet verbessern? Bitte wählen Sie einen oder mehrere Punkte aus der Liste aus. a) Die Benutzung eines Proxys. Cookies immer annehmen. b) Den Internetbrowserverlauf löschen. c) d) Keine persönlichen Daten preisgeben. e) Ich weiß es nicht. (Lösung: a, c, d) Wofür sind Proxys sinnvoll? Bitte wählen Sie einen oder mehrere Punkte aus der Liste aus. a) Um die eigene IP-Adresse zu verstecken. b) Um mittels Caching die Zugriffszeit auf Webseiten zu beschleunigen. c) Um unerwünschte Webseiten zu blockieren. d) Um den Standort des Computers zu verstecken. e) Ich weiß es nicht. (Lösung: a, b, c, d)
Verhaltensabsicht	Stellen Sie sich bitte nun vor: **Ihre sensiblen Patientendaten** können **verschlüs-**

(Intention), Cloud Computing im Gesundheitswesen zu akzeptieren	**selt in Einzelfragmenten über unterschiedliche Cloud-Anbieter** aus Ihrer aktuellen an die weiterbehandelnde medizinische Einrichtung (z.B. Krankenhaus oder Arztpraxis) **zum richtigen Zeitpunkt** übermittelt und dort rekonstruiert werden. Diese Fragmente ergeben **nur in einer bestimmten Anzahl** zusammen Ihre verschlüsselten Patientendaten und geben **andernfalls absolut nichts darüber** preis. Somit kann kein einzelner Cloud-Anbieter auf Ihre verschlüsselten Daten zugreifen und auch kleine Gruppen von Cloud-Anbietern nicht. Inwieweit wären Sie bereit, unter den oben beschriebenen Voraussetzungen der Übermittlung Ihrer Patientendaten zuzustimmen, wenn ... ... Ihre Patientendaten **sonst nicht rechtzeitig** beim Empfänger ankommen könnten. ... es sich um einen **Notfall** handelt. ... Ihre Patientendaten **sonst per Fax** übermittelt werden könnten. ... Ihre Patientendaten **sonst per Taxi** übermittelt werden könnten. ... **Sie sich selber darum kümmern** müssten. ... **der aus Ihrer Sicht sensible Teil** Ihrer **Patientendaten nicht mit übermittelt** wird. ... Ihre Patientendaten **vor der Verschlüsselung pseudonymisiert** (unter Verwendung eines Pseudonyms anstatt von Ihren personenidentifizierenden Daten) werden. Antwortmöglichkeiten: 1: Gar nicht bereit. 2: Weitgehend nicht bereit. 3: Eher nicht bereit. 4: Weder noch. 5: Eher bereit. 6: Weitgehend bereit. 7: Vollständig bereit.

Table 29. Research Model Constructs and Related Questionnaire Items (in German)

11.3 Security and Privacy-Preserving Architecture for Health Clouds

11.3.1 Rabin's Information Dispersal Algorithm: Share

```
package ida;
public class Share {
	private int x;
	private int[] y;
	public Share(int x, int[] y){
		this.x = x;
		this.y = y;
	}
	public int getX(){
		return x;
	}
	public int[] getY(){
		return y;
```

```
        }
}
```

(Ermakova, 2011, p. 78)

11.3.2 Rabin's Information Dispersal Algorithm: Dispersal

```
package ida;
import java.util.ArrayList;
public class Dispersal {
        private int prime;
        private String document;
        private int threshold; //m
        private int numberOfShares;
        private byte[] documentBytes;
        private int documentLength;
        public Dispersal (String document, int threshold, int numberOfShares, int prime) {
                this.document = document;
                this.threshold = threshold;
                this.numberOfShares = numberOfShares;
                this.prime = prime;
        }
        public ArrayList<Share> disperse()
        {
                documentBytes = document.getBytes();
                documentLength = documentBytes.length; //N
                if (! (documentLength % threshold == 0)) {
                        do {
                        document = document + 0;
                        documentBytes = document.getBytes();
                        documentLength = documentBytes.length; //N
                        } while (! (documentLength % threshold == 0));
                }
                int[][] F = new int[numberOfShares][documentLength/threshold];
                F = multiplyTwoMatrices(generateVandermondeMatrix(numberOfShares), generateMa-
trixFromDocumentBytes());
                ArrayList<Share> shares = new ArrayList<Share>();
                for(int i = 0; i < numberOfShares; i++) {
                        int[] y = new int[documentLength/threshold];
                        for(int j = 0; j < documentLength/threshold; j++) {
                                y[j] = F[i][j];
```

```
                        }
                        shares.add(new Share(i+1, y));
                }
                return shares;
        }
        private int[][] generateVandermondeMatrix (int numberOfShares) {
                int[][] VandermondeMatrix = new int[numberOfShares][threshold];
                for(int i = 0; i < numberOfShares; i++) {
                        for(int j = 0; j < threshold; j++) {
                                VandermondeMatrix[i][j] = (int) Math.pow((double) (i+1), (double) (j)) %
prime;
                        }
                }
                return VandermondeMatrix;
        }
        private int[][] generateMatrixFromDocumentBytes () {
                int[][] M = new int[threshold][documentLength/threshold];
                for (int i = 0; i < documentLength/threshold; i++) {
                        for (int j = 0; j < threshold; j++) {
                                M[j][i] = (int) documentBytes[i * threshold + j] & 0xFF;
                        }
                }
                return M;
        }
        private int[][] multiplyTwoMatrices (int[][] x, int[][] y) {
                int n = x.length;
                int m = x[0].length;
                // int m = y.length;
                int s = y[0].length;
                int[][] z = new int[n][s];
                for(int i = 0; i < n; i++) {
                        for (int k = 0; k < s; k++) {
                                for (int j = 0; j < m; j++) {
                                        z[i][k] = (z[i][k] + (x[i][j] * y[j][k]) % prime) % prime;
                                }
                        }
                }
                return z;
        }
}
```

(Ermakova, 2011, pp. 79-81)

11.3.3 Rabin's Information Dispersal Algorithm: Recovery

```
package ida;
import java.util.ArrayList;
public class Recovery {
	private int prime;
	private ArrayList<Share> shares;
	private int threshold;
	public Recovery(ArrayList<Share> shares, int threshold, int prime) {
		this.shares = shares;
		this.threshold = threshold;
		this.prime = prime;
	}
	public String recover() {
		// Generate matrix F from y values and the Vandermonde matrix from x values
		int yLength = shares.get(0).getY().length;
		int[][] F = new int[threshold][yLength];
		int[] x = new int[threshold];
		for (int i = 0; i < threshold; i++) {
			for (int j = 0; j < yLength; j++) {
				F[i][j] = shares.get(i).getY()[j];
			}
			x[i] = shares.get(i).getX();
		}
		// Calculate matrix M as multiplication of the inverse of the Vandermonde matrix and matrix F
		int M[][] = multiplyTwoMatrices(generateMatrixInverse(generateVandermondeMatrix(x)), F);
// A^{-1}*F = M = R
		// M -> doc
		return generateDocumentFromMatrix(M);
	}
	private String generateDocumentFromMatrix (int[][] M) {
		byte[] docBytes = new byte[M.length * M[0].length];
		int k = 0;
		for (int j = 0; j < M[0].length; j++) {
			for (int i = 0; i < M.length; i++) {
				docBytes[k] = (byte) M[i][j];
				k++;
			}
		}
```

```
                String document = new String (docBytes);
                return document;
        }
        private int[][] generateVandermondeMatrix (int[] x) {
                int xLength = x.length;
                int[][] VandermondeMatrix = new int[xLength][threshold];
                for (int i = 0; i < xLength; i++){
                        for (int j = 0; j < threshold; j++){
                                VandermondeMatrix[i][j] = (int) Math.pow((double) (x[i]), (double) (j)) %
prime;
                        }
                }
                return VandermondeMatrix;
        }
        private int[][] generateMatrixInverse(int[][] A) {
                // by Gauss-Jordan elimination
                int[][] MatrixInverse = new int[threshold][threshold];
                // Augmenting matrix A (threshold x threshold) with the Identity Matrix (threshold x threshold),
i.e. [AI] = M
                int[][] M = new int[threshold][2 * threshold];
                for (int i = 0; i < threshold; i++) {
                        for (int j = 0; j < threshold; j++) {
                                M[i][j] = A[i][j];
                                if (i == j) M[i][j + threshold]=1;
                        }
                }
                int d; int r;
                for (int i = 0; i < M.length; i++) {
                        d = M[i][i];
                        for (int k = 0; k < M[0].length; k++) {
                                M[i][k] = (M[i][k] * getMultiplicativeInverse(d, prime)) % prime;
                        }
                        for (int j=0; j<M.length; j++) {
                                if(j!=i) {
                                        r= M[j][i];
                                        for (int k = 0; k < M[0].length; k++) {
                                                M[j][k] = (prime + M[j][k] - (r * M[i][k]) % prime) %
prime;
                                                while (M[j][k] < 0) M[j][k] = M[j][k] + prime;
                                        }
                                }
```

```
                }
            }
            for (int i = 0; i < threshold; i++) {
                for (int j = 0; j < threshold; j++) {
                    MatrixInverse[i][j] = M[i][j + threshold];
                }
            }
        return MatrixInverse;
        }
        private int getMultiplicativeInverse(int b, int n) {
            int r1 = n; int r2 = b;
            int t1 = 0; int t2 = 1;
            int q, r, t;
            while (r2 > 0)
            {
                q = (r1 - r1 % r2) / r2;
                r = r1 - q * r2;
                r1 = r2;
                r2 = r;
                t = t1 - q * t2;
                t1 = t2;
                t2 = t;
            }
            while (t1 < 0) t1 = t1 + prime;
            return t1;
        }
        private int[][] multiplyTwoMatrices(int[][] x, int[][] y) {
            int n = x.length;
            int m = x[0].length;
                // int m = y.length;
            int s = y[0].length;
            int[][] z = new int[n][s];
            for(int i = 0; i < n; i++) {
                for(int k = 0; k < s; k++) {
                    for(int j = 0; j < m; j++) {
                        z[i][k] =(z[i][k] + x[i][j] * y[j][k]) % prime;
                    }
                }
            }
            return z;
```

```
        }
}
```

(Ermakova, 2011, pp. 81-84)

11.3.4 Rabin's Information Dispersal Algorithm: Main

```
package ida;
import java.util.ArrayList;
public class IDA {
        final int PRIME = 257;
        public IDA() {
        }
        public ArrayList<Share> getSharesFromDocument (String document, int threshold, int numberOf-
Shares){
                Dispersal dispersal = new Dispersal (document, threshold, numberOfShares, PRIME);
                return dispersal.disperse();
        }
        public String getDocumentFromShares (ArrayList<Share> shares, int threshold){
                Recovery recovery = new Recovery (shares, threshold, PRIME);
                return recovery.recover();
        }
}
```

(Ermakova, 2011, pp. 78-79)

11.3.5 Shamir's Secret-Sharing Scheme: Share

```
package ssss;
import java.math.BigInteger;
public class Share {
        private BigInteger x;
        private BigInteger y;
        public Share(BigInteger x, BigInteger y){
                this.x = x;
                this.y = y;
        }
        public BigInteger getX(){
                return x;
        }
        public BigInteger getY(){
```

```
		return y;
	}
	public void setY(BigInteger value){
		y = value;
	}
}
```

(Ermakova, 2011, pp. 84-85)

11.3.6 Shamir's Secret-Sharing Scheme: Dispersal

```
package ssss;
import java.math.BigInteger;
import java.util.ArrayList;
import java.util.Random;
public class Dispersal {
		private BigInteger prime;
		private String document;
		private int threshold;
		private int numberOfShares;
		public Dispersal (String document, int threshold, int numberOfShares, BigInteger prime) {
			this.document = document;
			this.threshold = threshold;
			this.numberOfShares = numberOfShares;
			this.prime = prime;
		}
		public ArrayList<Share> disperse() {
			ArrayList<Share> shares = new ArrayList<Share>();
			Random random = new Random();
			byte[] docBytes = document.getBytes();
			BigInteger[] coefficients = new BigInteger[threshold];
			coefficients[0] = new BigInteger(docBytes);
			for (int j = 1; j < threshold; j++) {
				byte[] coefBytes = new byte[docBytes.length];
				random.nextBytes(coefBytes);
				coefficients[j] = new BigInteger(coefBytes);
			}
			for (int j = 0; j < numberOfShares; j++) {
				byte[] xBytes = new byte[docBytes.length];
				random.nextBytes(xBytes);
				BigInteger x = new BigInteger(new Integer(j+1).toString());
```

```
                    BigInteger y = evaluate(coefficients, x);
                    shares.add(new Share(x, y));
                }
                return shares;
        }
        private BigInteger evaluate (BigInteger[] coefficients, BigInteger x) {
                BigInteger y = BigInteger.ZERO;
                for (int i = 0; i < coefficients.length; i++) {
                    y = y.add(coefficients[i].multiply(x.modPow(new BigInteger((new Inte-
ger(i)).toString()), prime)));
                }
                return y.mod(prime);
        }
}
```

(Ermakova, 2011, pp. 86-87)

11.3.7 Shamir's Secret-Sharing Scheme: Recovery

```
package ssss;
import java.util.ArrayList;
public class Recovery {
    private int prime;
    private int threshold;
    private ArrayList<Share> shares;
    public Recovery(ArrayList<Share> shares, int threshold, int prime) {
        this.shares = shares;
        this.threshold = threshold;
        this.prime = prime;
    }
    public String recover(){
        int[] x = new int[threshold];
        for (int j = 0; j < threshold; j++) {
            x[j] = shares.get(j).getX();
        }
        byte[] documentBytes = new byte[shares.get(0).getY().length];
        for(int i = 0; i < shares.get(0).getY().length; i++) {
            int[] y = new int[threshold];
            for (int j = 0; j < threshold; j++) {
                y[j] = shares.get(j).getY()[i];
            }
```

```
                documentBytes[i] = (byte) interpolate(x,y);
            }
            String document = new String (documentBytes);
            return document;
        }
        private int interpolate(int[] x, int[] y) {
            int retVal = 0;
            int desiredPosition = 0;
            for(int i = 0; i < x.length; i++) {
                int weight = 1;
                for(int j = 0; j < x.length; j++) {
                    if (j != i) {
                        weight = (weight * ((x[j] - desiredPosi-
tion)*getMultiplicativeInverse((prime+x[j] - x[i])%prime, prime))%prime)%prime;
                    }
                }
                retVal = (retVal + (weight * y[i])%prime)%prime;
            }
            return retVal;
        }
        private int getMultiplicativeInverse(int b, int n) {
            int r1 = n; int r2 = b;
            int t1 = 0; int t2 = 1;
            int q, r, t;
            while (r2 > 0) {
                q = (r1 - r1%r2)/r2;
                r = r1 - q * r2;
                r1 = r2;
                r2 = r;
                t = t1 - q * t2;
                t1 = t2;
                t2 = t;
            }
            while (t1 < 0) t1 = t1 + prime;
            return t1;
        }
}
```

(Ermakova, 2011, pp. 87-88)

11.3.8 Shamir's Secret-Sharing Scheme: Main

```
package ssss;
import java.math.BigInteger;
import java.util.ArrayList;
public class Recovery {
	private BigInteger prime;
	private int threshold;
	private ArrayList<Share> shares;
	public Recovery(ArrayList<Share> shares, int threshold, BigInteger prime) {
		this.shares = shares;
		this.threshold = threshold;
		this.prime = prime;
	}
	public String recover() {
		BigInteger[] x = new BigInteger[threshold];
		BigInteger[] y = new BigInteger[threshold];
		for (int j = 0; j < threshold; j++) {
			x[j] = shares.get(j).getX();
			y[j] = shares.get(j).getY();
		}
		String document = new String (interpolate(x,y).toByteArray());
		return document;
	}
	private BigInteger interpolate(BigInteger[] x, BigInteger[] y) {
		BigInteger retVal = BigInteger.ZERO;
		BigInteger desiredPosition = BigInteger.ZERO;
		for(int i = 0; i < x.length; i++){
			BigInteger weight = BigInteger.ONE;
			for(int j = 0; j < x.length; j++){
				if (j != i) {
					BigInteger top = x[j].subtract(desiredPosition);
					BigInteger bottom = x[j].subtract(x[i]);
					BigInteger curWeight = top.multiply(bottom.modInverse(prime));
					weight = weight.multiply(curWeight);
				}
			}
			retVal = retVal.add(weight.multiply(y[i]));
		}
		return retVal.mod(prime);
```

```
        }
}
```

(Ermakova, 2011, pp. 85-86)

11.3.9 Experiment

```
import ida.IDA;
//import ssss.SSSS;
import ida.Share;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.Date;
public class Experiment {
        public static void main(String[] args) {
                String str512kb = new String(" "); // insert a 512-KB string
                int threshold = 4;
                int numberOfShares = 4;
                String documentToDisperse = str512kb;
                ArrayList<Share> shares = disperse(documentToDisperse, threshold, numberOfShares);
                String documentObtained = recover(shares, threshold);
                byte[] documentBytes = documentToDisperse.getBytes();
                int documentLength = documentBytes.length; //N
                if (! (documentLength % threshold == 0)) {
                        do {
                        documentToDisperse = documentToDisperse + 0;
                        documentBytes = documentToDisperse.getBytes();
                        documentLength = documentBytes.length; //N
                        } while (! (documentLength % threshold == 0));
                }
        }
        public static ArrayList<Share> disperse(String documentToDisperse, int threshold, int numberOf-
Shares) {
                IDA idad = new IDA();
                //SSSS sssd = new SSSS();
                ArrayList<Share> shares = new ArrayList<Share>();
                int numberOfExperiments = 10000;
                double[] time = new double[numberOfExperiments];
                for(int i=0; i<numberOfExperiments; i++) {
                        Date date1 = new Date();
                        long start = date1.getTime();
```

```
                    shares = idad.getSharesFromDocument(documentToDisperse, threshold, numberOf-
Shares);
                    //shares = sssd.getSharesFromDocument(documentToDisperse, threshold, numberOf-
Shares);
                    Date date2 = new Date();
                    long end = date2.getTime();
                    time[i]= (double) (end-start);
                }
                computeStatistics(time);
                return shares;
        }
        public static String recover(ArrayList<Share> shares, int threshold) {
                String text = new String("");
                IDA idar = new IDA();
                //SSSS sssr = new SSSS();
                int numberOfExperiments = 10000;
                double[] time = new double[numberOfExperiments];
                for(int i=0; i<numberOfExperiments; i++) {
                        Date date1 = new Date();
                        long start = date1.getTime();
                        text = idar.getDocumentFromShares(shares, threshold);
                        //text = sssr.getDocumentFromShares(shares, threshold);
                        Date date2 = new Date();
                        long end = date2.getTime();
                        time[i]= (double) (end-start);
                }
                computeStatistics(time);
                return text;
        }
        public static void computeStatistics(double[] time) {
                double sum = 0;
                double mean = 0;
                double sumOfSquaredDeviations = 0;
                double standardDeviation = 0;
                double median = 0;
                for(int i=0; i<time.length; i++) {
                        sum = sum + time[i];
                }
                mean = sum/time.length;
                for(int i=0; i<time.length; i++) {
                        sumOfSquaredDeviations = Math.pow((mean - time[i]), 2);
```

```
                }
                standardDeviation = Math.sqrt(sumOfSquaredDeviations/sum);
                Arrays.sort(time);
                int middle = time.length/2;
                if (time.length%2 == 1) {
                        median = time[middle];
                }
                else {
                        median = (time[middle-1] + time[middle])/2;
                }
                System.out.println("mean = " + mean + "; standard deviation = " + standardDeviation + ";
median = " + median);
        }
}
```

(Ermakova, 2011, pp. 88-91)