Security and Privacy Requirements for Cloud Computing in Healthcare: Elicitation and Prioritization from a Patient Perspective

6

TATIANA ERMAKOVA, Weizenbaum Institute for the Networked Society & Fraunhofer FOKUS
BENJAMIN FABIAN, HfT Leipzig & Humboldt University of Berlin
MARTA KORNACKA, Humboldt University of Berlin
SCOTT THIEBES and ALI SUNYAEV, Karlsruhe Institute of Technology

Cloud computing promises essential improvements in healthcare delivery performance. However, its wide adoption in healthcare is yet to be seen, one main reason being patients' concerns for security and privacy of their sensitive medical records. These concerns can be addressed through corresponding security and privacy requirements within the system engineering process. Despite a plethora of related research, security and privacy requirements for cloud systems and services have seldomly been investigated methodically so far, whereas their individual priorities to increase the system success probability have been neglected. Against this background, this study applies a systematic requirements engineering process: First, based on a systematic literature review, an extensive initial set of security and privacy requirements is elicited. Second, an online survey based on the best-worst scaling method is designed, conducted, and evaluated to determine priorities of security and privacy requirements.

Our results show that confidentiality and integrity of medical data are ranked at the top of the hierarchy of prioritized requirements, followed by control of data use and modification, patients' anonymity, and patients' control of access rights. Availability, fine-grained access control, revocation of access rights, flexible access, clinicians' anonymity, as well as usability, scalability, and efficiency of the system complete the ranking. The level of agreement among patients is rather small, but statistically significant at the 0.01 level.

The main contribution of the present research comprises the study method and results highlighting the role of strong security and privacy and excluding any trade-offs with system usability. Enabling a richer understanding of patients' security and privacy requirements for adopting cloud computing in healthcare, these are of particular importance to researchers and practitioners interested in supporting the process of security and privacy engineering for health-cloud solutions. It further represents a supplement that can support time-intensive negotiation meetings between the requirements engineers and patients.

Authors' addresses: T. Ermakova, Weizenbaum Institute for the Networked Society, Hardenbergstraße 32, 10623 Berlin, Germany; Competence Center of Electronic Safety and Security Systems for the Public and Industries (ESPRI), Fraunhofer Institute for Open Communication Systems (FOKUS), Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany; email: tatiana.ermakova@fokus.fraunhofer.de; B. Fabian, Chair of Business Intelligence und Data Science, Hochschule für Telekommunikation Leipzig, Gustav-Freytag-Straße 43 - 45, 04277 Leipzig, Germany; email: fabian@hft-leipzig.de; B. Fabian and M. Kornacka, Institute of Information Systems, Humboldt University of Berlin, Spandauer Str. 1, 10178 Berlin, Germany; emails: bfabian@wiwi.hu-berlin.de, marta.kornacka@hotmail.com; S. Thiebes and A. Sunyaev, Department of Economics and Management, Institute for Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology, Kaiserstraße 12, 76131 Karlsruhe, Baden-Württemberg, Germany; emails: {scott.thiebes, sunyaev}@kit.edu.

2158-656X/2020/05-ART6 $15.00
https://doi.org/10.1145/3386160

CCS Concepts: • **Security and privacy → Software security engineering**; • **Networks → Cloud computing**; • **Applied computing → Health care information systems**;

Additional Key Words and Phrases: Cloud computing, healthcare, privacy, requirements, security

ACM Reference format:
Tatiana Ermakova, Benjamin Fabian, Marta Kornacka, Scott Thiebes, and Ali Sunyaev. 2020. Security and Privacy Requirements for Cloud Computing in Healthcare: Elicitation and Prioritization from a Patient Perspective. *ACM Trans. Manage. Inf. Syst.* 11, 2, Article 6 (May 2020), 29 pages.
https://doi.org/10.1145/3386160

1 INTRODUCTION

The McKinsey Global Institute estimates cloud computing to be among the top four technologies in terms of worldwide economic impact by 2025 [Manyika et al. 2013]. Cloud computing is an information technology (IT) service paradigm where virtual machines, development tools, and software are delivered on demand [Sunyaev 2020; Yang and Tate 2012; Mell and Grance 2011], usually over the Internet [Griebel et al. 2015]. Especially in the healthcare industry, the adoption of cloud computing has the potential to be a major transformative factor, as it is already changing conventional healthcare service delivery today [Benlian et al. 2018; Griebel et al. 2015; Sultan 2014a, 2014b; Hsieh et al. 2013; Ahuja et al. 2012; Kuo 2011]. Cloud computing supports collaboration between different healthcare stakeholders by enabling availability of medical data whenever and wherever they are required [Gao and Sunyaev 2019; Banerjee et al. 2016; Gao et al. 2016; Melício Monteiro et al. 2016; Weng et al. 2016; Fabian et al. 2015a; Lin et al. 2014a; Puustjärvi and Puustjärvi 2013; Nagarajan and Sukanesh 2012]. It is also regarded as a key technology for the delivery of patient-centered health IT applications, such as, for example, cloud-based appointment booking systems, directly accessible by patients and their relatives [Gao et al. 2018; Lin et al. 2014b]. To this end, recent empirical evidence demonstrates significant improvements regarding repetitive medical procedures [Eftekhari et al. 2017; Banerjee et al. 2016; Fujita et al. 2013], self-care [Kao et al. 2015; Piette et al. 2011], and completeness of medical records [Haskew et al. 2015] due the application of cloud computing.

However, despite the benefits of utilizing cloud computing in healthcare, leakage of medical data from the cloud might have serious consequences for patients such as, for instance, harassment by healthcare product marketers, or discrimination by employers, healthcare insurance agencies, and associates [Fabian et al. 2015b; Appari and Johnson 2010; Bansal et al. 2010; Laric et al. 2009; Rohm and Milne 2004]. Since patients are to be regarded as the legal owners and the center of authorizing the use of their sensitive medical data in the clinical practice [Karanasiou and Douilhet 2016; HHS 2000], they have a strong influence on and might even exert veto power over the deployment of the apparently beneficial cloud-based healthcare solutions [Zhang and Liu 2010]. With this regard and looking at online health information disclosure, researchers repeatedly confirmed that security and privacy concerns negatively impact patients' attitudes [Dinev et al. 2012; Lafky and Horan 2011], intentions regarding the service [Ermakova et al. 2016, 2014; Anderson and Agarwal 2011; Bansal et al. 2010; Bansal and Davenport 2010; Whetstone and Goldsmith 2009; Bansal et al. 2007; Angst et al. 2006], and actual behavior [Kuo et al. 2013]. Adding to this, recent scandals such as the unintended use of Facebook users' data by Cambridge Analytica [Cadwalladr and Graham-Harrison 2018] have spurred the public's concerns over the online disclosure and use of personal data. Thus, and because of the involvement of third-party cloud providers, security and privacy issues [Sajid and Abbas 2016; Abbas and Khan 2014; Latif et al. 2014; Kuo 2011] and related health information security and privacy concerns among patients [Ion et al. 2011; Ancker et al. 2012b,

2012a; Perera et al. 2011; Simon et al. 2009] are often reported as main barriers for the broad adoption of cloud-based applications in healthcare [Ermakova et al. 2016, 2014; Dinev et al. 2012; Anderson and Agarwal 2011; Lafky and Horan 2011; Bansal et al. 2010; Bansal and Davenport 2010; Whetstone and Goldsmith 2009; Bansal et al. 2007; Angst et al. 2006].

Concerns for information privacy are commonly related to the collection, unauthorized secondary use (internal and external), errors, and unauthorized access of information [Smith et al. 1996]. They can be generally supported through the fair information practice principles by the U.S. Federal Trade Commission, namely, notice, choice, access, and security [Bansal et al. 2008]. In the healthcare context, these are further reflected in the principles of "information and education" and "respect for patients' preferences" [Gerteis 1993] of the advocated patient-centered care notion [Gerteis 1993; Neugebauer et al. 2008]. These guidelines can be and in specific implementation scenarios (e.g., a new cloud service is ought to be introduced to a hospital) should be already considered within the system engineering process. Indeed, prior work highlights patients' lower privacy concerns in the presence of trust in the underlying privacy-preserving technologies [Ermakova et al. 2014; Dinev et al. 2012] and higher acceptance of cloud computing in healthcare under stronger health information protection [Ermakova et al. 2016], which can only be achieved through consideration and systematic analysis of patients' information security and privacy requirements.

Nevertheless, in the field of cloud computing in healthcare, only few publications systematically elicit and analyze security and privacy requirements [Ermakova et al. 2013a; Rodrigues et al. 2013; Deng et al. 2011; Zhang and Liu 2010]. Moreover, a strict requirements' hierarchy and relative importance of elicited requirements (especially from the patients' perspective) are left untouched [Dehling and Sunyaev 2014; Ermakova et al. 2013b]. Prioritized requirements are important for planning the development steps, software releases, and resources, as well as crucial for reducing the probability of system rejection [Achimugu et al. 2014; Sperling 2009]. The present study attempts to partly close this research gap, by providing answers to the following research questions: (1) What are security and privacy requirements for cloud computing in healthcare? (2) What is the relative importance of identified security and privacy requirements as perceived by patients? To answer the above research questions, this study leans on a well-established systematic and user-oriented requirements engineering framework in information systems development, which calls for requirements elicitation, analysis, and prioritization with direct involvement of users [Sommerville and Sawyer 1997]. First, a list of updated security and privacy requirements for cloud computing in the healthcare sector is derived and analyzed based on a comprehensive literature review [vom Brocke et al. 2015, 2009; Levy and Ellis 2006; Webster and Watson 2002]. This technique was preferred over any user-to-analyst (researcher) communications, which would have been more limited in scope [Burnay 2016; Davey and Parker 2015; Beg et al. 2008; Appan and Browne 2012]. Second, to prioritize the derived security and privacy requirements, an online survey based on the best-worst scaling (BWS) method [Finn and Louviere 1992] is designed, conducted, and evaluated. With BWS for pairwise comparisons, patients revealed their preferences with relatively few questions over the set of security and privacy requirements for cloud computing in healthcare, without being in need to make fine-grained distinctions [Cohen et al. 2009; Lee et al. 2007; Marley and Louviere 2005; Cohen 2003; Finn and Louviere 1992]. Moreover, pairwise comparisons are preferred to numerical assignments [Achimugu et al. 2014] for more informative and accurate results [Karlsson 1996].

The article is organized as follows: Section two provides related work in the context of the present study. Sections three and four present the research method and the results of the two-staged systematic requirements engineering process, respectively. Section five discusses the principle findings of the study, describes its limitations and implications for research and practice, and suggests directions for future research, before section six outlines conclusions.

Table 1. Related Literature

Stream of Related Literature	Past Research Foci	Exemplary Literature
Security and privacy (threats) of online sharing of healthcare information	Security and privacy threats to online-processed health information	Thiebes et al. [2017] and Rindfleisch [1997]
	Security and privacy issues related to the exchange of electronic health records between healthcare organizations	van der Linden et al. [2009]
	Security and privacy requirements for centralized electronic health records	Wainer et al. [2008]
Technical design of and privacy-enhancing mechanisms for cloud-based health applications, infrastructures, and platforms	Technical aspects of access control	Li et al. [2010], Yu et al. [2010], Chen and Hoang [2011], Basu et al. [2012], Chen et al. [2012a, 2012b], and Li et al. [2012]
	Audit and tracing mechanisms	Nematzadeh and Camp [2010]
	Encryption and authorization	Li et al. [2011b]
	Security of client platforms	Löhr et al. [2010]
	Privacy-preserving protocols	De Decker et al. [2008]
Security and privacy requirements for cloud-based health applications	Requirements elicitation based on case scenarios and business logic	Deng et al. [2011] and Zhang and Liu [2010]
	Pure literature reviews on security and privacy requirements	Rodrigues et al. [2013]
	Literature- and scenario-driven elicitation of security and privacy requirements	Ermakova et al. [2013a]

2 RELATED LITERATURE

2.1 Information Security and Information Privacy

Within this research, our focus is on information security and information privacy, as opposed to, for example, physical security and privacy. Security and privacy are both associated with the protection of information as well as the systems and hardware involved in the usage, storage, and transmission of that information [Andress 2014, p. 3]. Although information security and information privacy are often not clearly differentiated [Dinev et al. 2013; Bansal and Zahedi 2010], we align our understanding of both concepts with Bansal and Zahedi [2010, p. 2], who mainly distinguish between privacy and security issues dependent on whether they result from the actions of the vendor or a third-party criminal: "[P]rivacy issues arise when the data are in the possession of the vendor and are the results of actions (or neglect) by the vendor, whereas security issues arise when the data are in either the transmission or possession state and abuse takes place as a result of the action by a third-party criminal."

2.2 Current State of Research on Security and Privacy Requirements for Cloud Computing in Healthcare

In the presence of severe security and privacy concerns in the age of online healthcare information technologies [Gao and Sunyaev 2019; Ancker et al. 2012a, 2012b; Lafky and Horan 2011; Perera et al. 2011; Simon et al. 2009; Whiddett et al. 2006], facilitating perceived efficacy of privacy-preserving technological mechanisms was shown to be an important means for reducing security and privacy concerns [Ermakova et al. 2014; Dinev et al. 2012], and thus strengthening health cloud acceptance [Gao and Sunyaev 2019; Ermakova et al. 2016].

We summarize relevant literature streams for our study, their past research foci, as well as exemplary literature for each stream in Table 1. While there is a plethora of extant research concerned

with security and privacy for cloud computing in healthcare, most of this research discusses security and privacy requirements rather parenthetically, as their actual focus lies on the technical aspects of access control [Li et al. 2010; Yu et al. 2010; Chen and Hoang 2011; Basu et al. 2012; Chen et al. 2012a, 2012b; Li et al. 2012], audit and tracing mechanisms [Nematzadeh and Camp 2010], encryption and authorization [Li et al. 2011b], the security of client platforms [Löhr et al. 2010], and privacy-preserving protocols [De Decker et al. 2008]. Only few studies follow a general and systematic requirements engineering framework for security and privacy requirements elicitation and analysis in the field of cloud computing in healthcare [Ermakova et al. 2013a; Rodrigues et al. 2013; Deng et al. 2011; Zhang and Liu 2010]. Deng et al. [2011] and Zhang and Liu [2010], for example, use case scenarios and business logic to elicit privacy and security requirements, while Rodrigues et al. [2013] derive a set of security and privacy requirements from Medline sources. The study by Ermakova et al. [2013a], however, combines both literature-driven and scenario-driven strategies. While certainly valuable, these studies however are more limited in scope than the literature review presented in this manuscript as they focus on specific scenarios in healthcare. Furthermore, these literature reviews have been conducted between 2010 and 2013, whereas it is likely that in the meantime new requirements have emerged or existing requirements have changed in the dynamic cloud computing field [Jarke and Lyytinen 2015]. Last, these studies do not investigate the relative importance of identified requirements, in particular not from patients' perspectives.

Although, insights into security and privacy in the field of cloud computing in healthcare can also be gained from publications with focus on security and privacy (threats) of online sharing of healthcare information in general [Thiebes et al. 2017; van der Linden et al. 2009; Wainer et al. 2008; Rindfleisch 1997], as well as the previously mentioned works devoted to the technical design of and privacy-enhancing mechanisms for concrete cloud-based health applications, infrastructures, and platforms [Chen et al. 2012a, 2012b; Deng et al. 2012; Shini et al. 2012; Abbadi et al. 2011; Chen and Hoang 2011; Deng et al. 2011; Li et al. 2010; Löhr et al. 2010; Yu et al. 2010], those works also do not account for the relative importance of security and privacy requirements from the patients' point of view.

3 PHASE 1: REQUIREMENTS ELICITATION AND ANALYSIS

This study is divided into two phases. In this first phase, we conducted a comprehensive review of literature on security and privacy requirements for cloud computing in healthcare [vom Brocke et al. 2015, 2009; Levy and Ellis 2006; Webster and Watson 2002]. A literature review is regarded as a superior technique over any constrained user-to-analyst communications [Burnay 2016; Davey and Parker 2015; Beg et al. 2008; Appan and Browne 2012]. Nevertheless, the rather dynamic nature of the cloud computing sector [Yang and Tate 2012] necessitates their regular validations and updates [Dehling and Sunyaev 2014].

3.1 Method

At the first search stage of the literature search process, as proposed by vom Brocke et al. [2009] and Levy and Ellis [2006], we searched in the AIS World MIS Journal Ranking list and the online databases IEEE Xplore, Emerald, Springer, ACM Digital Library, AIS Electronic Library (AISeL), Proquest, EBSCOhost, and ScienceDirect [Levy and Ellis 2006], for all possible keyword combinations of the terms: "security," "secure," "privacy," "requirements," "health cloud," "cloud-based healthcare," "electronic healthcare," "e-health," "electronic health records," and "personal health records." As Gartner Research mentioned cloud computing among the top technologies for the first time in 2010 [Sahlin 2013], and since we want to focus on only up-to-date findings, we set 2010 as the starting year for our searches. At the second stage of the literature search process, the

querying was restricted to literature stating specific security and privacy requirements. All article hits were evaluated for their potential relevance based on their abstracts, titles, and, if necessary, full texts. Additionally, a backward and forward search [vom Brocke et al. 2015, 2009; Levy and Ellis 2006; Webster and Watson 2002] was conducted. Finally, out of all 48,180 hits, we rejected 48,150 articles, because they were either off topic or did not specify any requirements. About 30 studies were classified as relevant for further analysis and contributed directly to the present study with precisely formulated security and privacy requirements.

3.2 Results

The requirements elicitation was based on mentions in the previously identified relevant studies. The requirements were first noted separately and then consolidated. Moreover, semantically comparable requirements were organized into groups for better illustration. Our groups were based on the CIA triad (confidentiality, integrity, and availability) [Fabian et al. 2010], however, without explicitly limiting them to this framework. Tables 2, 3, and 4 provide an overview of the final set of derived requirements, their definitions in a natural language as suggested by Rupp [2005], as well as the respective studies each requirement originated from.

3.2.1 Requirements Related to Confidentiality of Medical Data. One of the most frequently mentioned security and privacy requirements in the literature is confidentiality of medical data (see Table 2). This rather abstract security goal from the CIA triad implies that medical data stored in the cloud should be accessible only to authorized users [Li et al. 2012; Stallings 2003; Shirey 2000]. It also entails that the system should prevent unauthorized data disclosure [Ermakova et al. 2013a; Chen et al. 2012a; Shirey 2000; Barrows and Clayton 1996].

With access control, access to medical data can be further limited via communication links [Stallings 2003]. In the given sensitive health-related context, the control of access rights by patients contributes to confidentiality by creating better transparency over access rights and authorized users. Additionally, it may convey a feeling of control over data [Gholami et al. 2014; Basu et al. 2012]. Revocation of access rights allows to withdraw access rights for certain users or schedule them to expire to a certain point of time [Shirey 2000], whenever medical data is no longer required (e.g., the family doctor at a previous place of treatment) [Basu et al. 2012]. With fine-grained access control to medical data, different users (e.g., medical workers) should receive different levels of access rights based on their role and information needs within the medical service delivery [Gholami et al. 2014; Li et al. 2012; Deng et al. 2011; Zhang and Liu 2010]. In practice, this could mean that a dentist would receive all information related to her or his patients' previous dental disorders and treatments and no mental ones. Flexible access to medical data, being intensively discussed [Basu et al. 2012; Barnickel et al. 2010; Li et al. 2010; Löhr et al. 2010; Wainer et al. 2008], enables clinicians to take timely measures and access medical data in exceptional or emergency cases, especially when a patient is unable to express her or his consent [Löhr et al. 2010].

The requirement of anonymity of patients and medical workers implies that these actors' true identities should remain unknown to unauthorized users [Deng et al. 2011; Li et al. 2011b]. Further, it means that information about their true identity should not be disclosed or traced back to them from system indexes or actions [Deng et al. 2011; Löhr et al. 2010; De Decker et al. 2008]. The unlinkability of medical data requires that the link between different medical actions and medical data pieces is invisible for unauthorized parties [Deng et al. 2011; De Decker et al. 2008]. Ownership of medical records in the cloud still constitutes a much debated legal issue [Zhang and Liu 2010]. Accordingly, clear information about who needs to be protected against medical data misuse [Chen et al. 2012b] or who is in charge of storing and creating the medical record [Shini et al. 2012] is necessary for an effective and target-oriented protection of cloud-based medical data [Chen et al. 2012b; Shini et al. 2012].

Table 2. Requirements Related to Confidentiality of Medical Data

Requirements	Definitions	Further Sources
Confidentiality of medical data	The system shall ensure that medical data can be accessed only by authorized users [Li et al. 2012].	[Ermakova et al. 2013a; Chen et al. 2012a; Li et al. 2012; Shini et al. 2012; Abbadi et al. 2011; Chen and Hoang 2011; Deng et al. 2011; Barnickel et al. 2010; Löhr et al. 2010; Zhang and Liu 2010; van der Linden et al. 2009; Wainer et al. 2008; Barrows and Clayton 1996]
Control of access rights to medical data by patients	The system shall enable patients to authorize other users to access their medical data [Basu et al. 2012].	[Basu et al. 2012; Chen et al. 2012a, 2012b; Li et al. 2012; Abbadi et al. 2011; Barnickel et al. 2010; Zhang and Liu 2010; van der Linden et al. 2009; Wainer et al. 2008]
Revocation of access rights to medical data	The system shall ensure that access can be revoked when not needed [Basu et al. 2012].	[Ermakova et al. 2013a; Basu et al. 2012; Chen et al. 2012a; Li et al. 2012, 2011b; Barnickel et al. 2010; Li et al. 2010; De Decker et al. 2008]
Fine-grained access control to medical data	The system shall ensure that users can access only a necessary amount of medical data [Li et al. 2012; Zhang and Liu 2010; Rindfleisch 1997].	[Ermakova et al. 2013a; Padmini et al. 2013; Li et al. 2012, 2011b, 2010; van der Linden et al. 2009; Wainer et al. 2008; Rindfleisch 1997]
Flexible access to medical data	The system shall enable sharing of medical data without patients' involvement or explicit consent (e.g., in emergency situations) [Löhr et al. 2010].	[Ermakova et al. 2013a; Basu et al. 2012; Barnickel et al. 2010; Li et al. 2010; Löhr et al. 2010; Wainer et al. 2008]
Anonymity of medical workers	The system shall ensure that medical workers' identity cannot be derived from medical data, indexes, or their actions in the system [Deng et al. 2011; Li et al. 2011b].	[Abbadi et al. 2011; Deng et al. 2011; Li et al. 2011a; Löhr et al. 2010; Nematzadeh and Camp 2010]
Anonymity of patients	The system shall ensure that patients' identity cannot be derived from the medical data, indexes, or their actions in the system [Ermakova et al. 2013a].	[Ermakova et al. 2013a; Deng et al. 2011]
Unlinkability	The system shall ensure that the link between different medical actions, medical data pieces, and identities will be hidden from unauthorized users [Deng et al. 2011; De Decker et al. 2008].	[Ermakova et al. 2013a; Abbadi et al. 2011; Deng et al. 2011; Li et al. 2011a; De Decker et al. 2008]
Ownership of medical data	The system shall define who is the owner, the creator and the manager of medical data [Zhang and Liu 2010].	[Ermakova et al. 2013a; Chen et al. 2012b; Barnickel et al. 2010; Zhang and Liu 2010; Barrows and Clayton 1996]

3.2.2 Requirements Related to Integrity of Medical Data. The next broadly defined requirement from the CIA triad is integrity of medical data (see Table 3). It assures that only authorized users are able to modify health records in the cloud [Chen et al. 2012b; Stallings 2003] and, hence, medical workers can fully rely on accuracy and consistency of medical data [Zhang and Liu 2010]. In general, correctness of medical data is of highest importance in clinical practice, since errors could cause life-threatening situations or require the repetition of painful and costly medical treatments [Israelson and Cankaya 2012; Deng et al. 2011]. Integrity of medical data should further be supported by the ability of the system to detect and protect itself from security attacks and violations [Chen and Hoang 2011]. To detect and track malicious behavior at the proper time, recording of users' actions and authentication can be taken into consideration [Zhang and Liu 2010; Barrows and Clayton 1996]. Finally, non-repudiation provides evidence that no user can falsely deny having

Table 3. Requirements Related to Integrity of Medical Data

Requirements	Definitions	Further Sources
Integrity of medical data	The system shall ensure that medical data can be changed only by authorized users [Chen et al. 2012b] to allow for accuracy and consistency of medical records [Zhang and Liu 2010].	[Gholami et al. 2014; Ermakova et al. 2013a; Basu et al. 2012; Shini et al. 2012; Abbadi et al. 2011; Deng et al. 2011; van der Linden et al. 2009; Barrows and Clayton 1996]
Detection and prevention of security attacks and violations	The system shall detect and prevent security attacks and violations [Chen and Hoang 2011].	[Ermakova et al. 2013a; Chen et al. 2012a, 2012b; Chen and Hoang 2011]
Auditability of users' actions	The system shall record and control users' actions, such as every data access or data modification [Zhang and Liu 2010].	[Gholami et al. 2014; Ermakova et al. 2013a; Basu et al. 2012; Chen et al. 2012b; Abbadi et al. 2011; Chen and Hoang 2011; Zhang and Liu 2010; van der Linden et al. 2009]
Authenticity and authentication of users	The system shall validate users' identities every time they access medical data [Zhang and Liu 2010].	[Ermakova et al. 2013a; Abbadi et al. 2011; Zhang and Liu 2010; van der Linden et al. 2009]
Non-repudiation of users' action	The system shall ensure users cannot deny they accessed medical data [van der Linden et al. 2009].	[Ermakova et al. 2013a; Chen et al. 2012a, 2012b; Löhr et al. 2010; Zhang and Liu 2010; van der Linden et al. 2009; Wainer et al. 2008]

Table 4. Requirements Related to Availability of Medical Data

Requirements	Definitions	Further Sources
Availability of medical data	The system shall ensure that medical data is available anytime [Chen et al. 2012b].	[Ermakova et al. 2013a; Basu et al. 2012; Shini et al. 2012; Abbadi et al. 2011; Deng et al. 2011; Ateniese et al. 2003; Rindfleisch 1997; Barrows and Clayton 1996]
Archiving and recoverability of medical data	The system shall ensure an offline back-up so that medical data can be restored to a specific point of time without any information loss [Zhang and Liu 2010].	[Ermakova et al. 2013a; Zhang and Liu 2010; van der Linden et al. 2009; Wainer et al. 2008; Rindfleisch 1997]
Robustness of the system	The system shall ensure that medical data is available despite system failures, power or Internet outages [Zhang and Liu 2010].	[Zhang and Liu 2010]
Up-to-dateness of medical data	The system shall ensure that the medical data is up-to-date [Wainer et al. 2008].	[van der Linden et al. 2009; Wainer et al. 2008]
Long-term storage of medical data	The system shall ensure that medical data can be stored for a long time [Chen et al. 2012b].	[Chen et al. 2012b; Zhang and Liu 2010; van der Linden et al. 2009; Wainer et al. 2008]
Usability, scalability and efficiency of the system	The system shall be efficient, easy in use and support storage of large medical data [Li et al. 2012, 2010; Wainer et al. 2008].	[Ermakova et al. 2013a; Huang et al. 2012; Li et al. 2012, 2011b, 2010; Wainer et al. 2008]

accessed the medical data [Zhang and Liu 2010; van der Linden et al. 2009; Stallings 2003; Shirey 2000].

3.2.3 Requirements Related to Availability of Medical Data. The availability requirement demands that medical data is accessible and usable upon demand [Stallings 2003; Shirey 2000], enabling quick provision of healthcare services (see Table 4). Archiving and recoverability of medical data ensures that medical data can be easily restored to a specific point of time without any loss of information [Zhang and Liu 2010; van der Linden et al. 2009; Wainer et al. 2008; Rindfleisch 1997].

Zhang and Liu [2010] also require that medical data is available despite system failures, and power or Internet outages. Further, electronic health records should be up to date and available with no delay [van der Linden et al. 2009; Wainer et al. 2008]. Long-time storage of medical records ensures that they can be viewed even after the patient's treatment is completed (e.g., for legal inquest of treatment failures) [Wainer et al. 2008; Chen et al. 2012b]. Finally, usability, scalability, and efficiency of the system are regarded in the literature as further related requirements. This stipulates that cloud-based healthcare systems should be efficient, easy to handle by end-users, and support storage of large medical data sets [Li et al. 2012, 2010].

4 PHASE 2: REQUIREMENTS PRIORITIZATION

In phase two, we designed, conducted, and evaluated an online survey based on the BWS method [Finn and Louviere 1992]. The BWS method enables disclosing patient preferences over the set of security and privacy requirements for cloud computing in healthcare within a relatively small number of questions and does not require fine-grained distinctions [Cohen et al. 2009; Lee et al. 2007; Marley and Louviere 2005; Cohen 2003; Finn and Louviere 1992]. Moreover, as a pairwise comparison technique, it gives a more informative and accurate requirement prioritization [Karlsson 1996], in contrast to a numerical assignment technique [Achimugu et al. 2014].

4.1 Method

4.1.1 Best-worst Scaling Method. The BWS method, or maximum difference scaling method, is an extension of Random Utility Theory for paired comparison judgements [Thurstone 1994]. It was introduced by Finn and Louviere [1992] to measure concerns or preferences of individuals, allowing for a full ranking of measured options [Cohen et al. 2009; Marley and Louviere 2005]. To that end, the BWS approach attempts to create trade-off choice situations that are easy to handle by the respondents. Within several rounds the respondents are requested to choose the best and the worst option per choice set, including combinations of different options from a large list [Cohen et al. 2009; Lee et al. 2007; Marley and Louviere 2005; Cohen 2003; Finn and Louviere 1992]. The best-worst choices underlie the MaxDiff model and the sequential choice model [Flynn et al. 2007; Marley and Louviere 2005]. According to the MaxDiff model, individuals choose the best-worst pair that provides the biggest difference in utility [Flynn et al. 2007; Finn and Louviere 1992]. In the sequential choice model, people choose the most preferred option first and then pick the least preferred alternative in the subset [Marley and Louviere 2005].

In general, the BWS method allows for three different forms of experiments (cases) depending on the number of attributes, attribute levels, or profiles of attributes with different levels to be ranked. The case 1 experiment (object case) focuses on respondents' preferences with respect to the list of options with one attribute level only. The case 2 experiment (profile case) allows for the analysis of options having more attribute levels. Last, the case 3 experiment (multi-profile case) collects data on people's preferences with respect to the attribute profiles with a varying attribute level [Kübler 2012; Marley and Louviere 2005].

The BWS method has a wide field of applications [Kübler 2012] and was already successfully used in market research and social sciences [Cohen et al. 2009; Auger et al. 2007; Finn and Louviere 1992], as well as in the area of cloud computing services to evaluate the relative importance of assurances and certifications [Lansing et al. 2013].

Various studies highlight the advantages of the BWS method in comparison to the traditional preference measurement approaches such as rating scales (e.g., a Likert scale) [Kübler 2012; Cohen et al. 2009; Marley and Louviere 2005]. In line with this, related to the most cited requirement prioritization techniques [Achimugu et al. 2014], Karlsson [1996] posited that in terms of informativeness and accuracy a pairwise comparison technique leading to the importance of requirements

is a more efficient means for selecting among candidate requirements, compared to a numerical assignment technique grouping requirements into different categories in correspondence with their level of importance, that is high, medium, and low. Indeed, BWS is expected to provide better and more reliable estimates, since it is less vulnerable to potential biases, changes in means, and variances [Lee et al. 2007; Baumgartner and Steenkamp 2001]. Since the BWS approach is scale-free, respondents are not able to constantly use certain parts of the rating scale [Lee et al. 2007; Cohen and Neira 2003; Cohen and Markowitz 2002]. Further, the BWS method forces people to make trade-offs and to discriminate between the options, since respondents need to consider the extreme values (best and worst) only [Flynn et al. 2007; Lee et al. 2007; Marley and Louviere 2005; Cohen and Markowitz 2002]. This is particularly useful when investigating people's preferences for security and privacy requirements, where people may tend to identify all requirements as most important [Firesmith 2004]. Additionally, the data collected within the BWS framework is expected to deliver the maximum amount of information including the most preferred requirement, the least preferred requirement, as well as individual and aggregated preference rankings of requirements [Kübler 2012; Marley and Louviere 2005]. Finally, collected data is easy to analyze and a full rank of requirements can be easily obtained by calculating the simple best-worst scores [Marley and Flynn 2014; Cohen et al. 2009; Marley and Louviere 2005].

4.1.2 Security and Privacy Requirements of Patients. Pairwise comparison techniques generally suffer from scalability problems [Achimugu et al. 2014]. Since too many items require too much effort for participants, best practices show that respondents are usually able to concentrate on between 10 and 12 choice sets including between four and six items [Cohen et al. 2009]. Therefore, BWS based on 11 choice sets was selected (see Table 6), with every choice set comprised of five requirements and each requirement appearing only twice with another requirement [Cochran and Cox 1957]. We therefore narrowed down the initial set of 20 literature-based requirements to be examined during the BWS survey according to the following rationale.

Security and privacy requirements often exhibit strong interdependencies, which also holds true for the 20 requirements presented in this article. Since such interdependencies might confound participants, we chose requirements for the BWS survey such that potential interdependencies are minimized. Accordingly, we first select confidentiality (1), integrity (4), and availability (10) of medical data to be included in the survey, as they represent the pillars of the widely established CIA triad.

Next, to these essential requirements, further confidentiality-enhancing requirements result from our sensitive health-related context. Specifically, additionally included requirements aim to support the fine-grained disclosure of medical data (i.e., fine-grained access control to medical data (8)), as well as preventing unauthorized disclosure at a later time period (i.e., revocation of access rights to medical data (11)), without patients' willingness (i.e., control of access rights to medical data by patients (3)), except for specified conditions (i.e., flexible access to medical data, or guarantee of access rights to medical data in emergency cases without patients' involvement (5)). In general, access control enables to limit access to medical data enforced through communication links [Stallings 2003]. Fine-grained access control to medical data (e.g., based on roles as in RBAC [Sandhu et al. 1996]), leads to a better reflection of the "need-to-know" principle as well as to enhanced confidentiality and integrity. Revocation of access rights to medical data could further improve long-term confidentiality and integrity by preventing access to the data by persons who are not authorized anymore. Control of access rights to medical data by patients presents a fundamental measure for patients to handle their health data according to their own preferences. However, at the same time, this requirement possesses a strong interdependency to the ownership of medical data requirement. Under the legislative frameworks such as Directive 95/46/EC of the

European Parliament and of the Council and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, patients' right to personal medical data protection overrides the property right notion [Karanasiou and Douilhet 2016]. Data ownership might therefore be a difficult-to-grasp concept and could also refer to different legal connotations among different study participants [Pleasence et al. 2015]. We also presume that study participants might become confused and wonder why there could be situations in which they do not own their data. Consequently, we decided to exclude the ownership of medical data requirement from the BWS survey. Flexible access to medical data (e.g., in emergencies without patients' involvement or to provide more efficient healthcare processes) results in important trade-offs with other security requirements.

Next, patients should not be identifiable in health data by unauthorized parties, and anonymity of patients (9) was thus also included in the BWS survey. Similarly, anonymity of medical workers (7) was included to reflect multilateral security, since medical workers may as well have (potential) anonymity requirements in health-data processing systems. However, the unlinkability requirement is semantically connected to unauthorized observability of both patients and medical workers, which is why it might be difficult to clearly differentiate from those requirements for some of our study's participants. Anonymity, considered as an "intuitive" concept among study participants, seems to capture the specifics of unlinkability quite well.

To ensure integrity, such measures as authenticity and authentication of users, non-repudiation and auditability of users' actions, detection and prevention of security attacks and violations must be in place [FFIEC 2008; Stallings 2003]. We subsumed these under control of use and modification of medical data (2) here for the following reasons. Control of use and modification of medical data is an important security measure especially for protecting confidentiality and integrity of the data, and detecting misuse. Authenticity and authentication of users are a priori requirements for control and use of modification that are geared toward system engineering. Their general goal is to support the prevention of the unauthorized access and modification of medical data. From a user perspective, control of use and modification of medical data can therefore be considered as the overarching goal of these requirements. Non-repudiation (e.g., of actions such as accessing and modifying patient data) is, from a user's perspective, part of the control of use and modification of medical data as it is semantically connected to the concept of control. Furthermore, the term might be unfamiliar to a general audience. Auditability can be seen as a more operational perspective on non-repudiation, and therefore also part of the control of use and modification of medical data. The term could also refer to different legal connotations among different study participants. Detection and prevention of security attacks and violations is a more technical requirement from systems (security) engineering, which has the ultimate goal of preventing unauthorized access and use of systems and data. From a patient's perspective, in can therefore be regarded as part of the control of use and modification of medical data.

Availability of medical data includes its availability also despite system, network or cloud failures [Fabian et al. 2015a; Stallings 2003], which is a central goal of robustness, as defined by IEEE Standard Glossary of Software Engineering Terminology [IEEE 1990]. As for up-to-dateness of medical data, availability can also be understood as implicitly referring to "fresh" and recent data, in contrast to outdated data of conceivably lower usefulness. Availability does not explicitly suppose an expiry date. Moreover, healthcare providers can be obliged to keep medical files for an established long-term retention period or even permanently [Rinehart-Thompson 2008], what would require them to move medical data no longer actively used to a separate storage device or archive [Shirey 2000]. Hence, archiving and recoverability is a more technical requirement from system engineering that has the goal of long-term availability. As such, long-term storage of medical data, and archiving and recoverability of medical data are only of indirect relevance for patients and, therefore, covered under availability in the present study. Finally, system usability, scalability, and

efficiency of the system (6) complete the list, as they could result in potential conflicts with the other included requirements. Such trade-offs are common results of security engineering decisions and system implementations, and have been reported to be important in security literature [Lampson 2009; Yee 2004].

Tables 9 and 10 in the Appendix summarize the previously described reasons for including and excluding individual requirements, respectively.

4.1.3 Online Survey Design. The online survey consisted of three main parts: framing, best-worst scaling choice sets (based on the case 1 experiment, see Section 4.1.1), and demographic questions including age, gender, profession, and medical working experience. Within the framing part, taking into account the complexity of the cloud computing term [Lin and Chen 2012], we provided some basic information on cloud computing and its potential applications in healthcare. In particular, cloud computing was referred to as the online usage of software services and storage capacities of remote computer centers (e.g., GoogleDocs, Webmail). Since survey respondents can better reveal their true preferences regarding real-life situations [Sommerville and Sawyer 1997], they were asked to consider a short cloud-based healthcare data sharing scenario equivalent to the example case used by Fabian et al. [2010] and derived from the scenario-driven analysis by Ermakova et al. [2013a]. The scenario reads as follows: *After a completed medical treatment, the patient is free to leave the hospital and move to the rehabilitation center. Therefore, the doctor in charge sends the patient's medical data (including medical history, diagnosis, prescribed medicines, and allergies) to the medical staff at the patient's new health center. Additionally, the nurse can add further information about other communicable diseases of the patient. This information exchange between the medical staff is enabled by the cloud.*

Hence, the scenario was only demonstrating the possible features of a cloud-based health IT service. Further, respondents were told to consider a list of 11 security and privacy requirements that a random cloud service provider commits to fulfill in a given scenario (see Table 5). In line with the recommendations by Rupp [2005] and Sommerville and Sawyer [1997], the requirements definitions were formulated informally and in a natural language to be easily understandable. To account for order effects, the order appearance of the requirements in the framing part, within the blocks and also of the blocks themselves was randomized [Cohen et al. 2009; Lansing et al. 2013] (see Table 6 for the order appearances within the blocks).

4.2 Results

4.2.1 Data Collection and Sample. The survey data was collected from January until the end of February 2015. Participants were mainly recruited via social networks and a newsletter at the Humboldt University of Berlin, who were encouraged to participate in the survey by freely entering a raffle for three amazon vouchers each worth €10. This focus on German participants was chosen, since Germans are known as being peculiarly concerned about their privacy [Bellman et al. 2004]. Out of 405 people who followed the hyperlink to the survey, 245 respondents fully completed it. People having a minimum of one year of working experience in the medical field were excluded from the study (16), to avoid confounding the patient-centric perspective with the viewpoint of those experienced in healthcare delivery [TAPAS 2004; Gürses et al. 2005; Gürses and Santen 2006; Fabian et al. 2010; Gürses et al. 2006; Ermakova et al. 2013a]. This resulted in a final sample of 229 patients. Of these 229 patients in the sample, 129 were females (56.33%) and 100 males (43.67%). A great majority of all respondents (184 or 80.35%) were aged between 21 and 30 years old, 24 (or 10.48%) were aged less than 20, 17 (or 7.42%) were in the age between 31 and 40, 2 (or 0.87%) were aged between 41 and 50, and the remaining two people provided no answer.

Table 5. Online Survey Requirements

Requirement	Related requirements (see Tables 2, 3, and 4)	Definition	Nr.
Anonymity of patients	*Anonymity of patients* and *Unlinkability* *Unlinkability*	The system shall ensure that the true identity of a patient cannot be derived from users' data and activities in the system.	9
Anonymity of medical workers	*Anonymity of medical workers* and *Unlinkability*	The system shall ensure that the true identity of a medical worker cannot be derived from users' data and activities in the system.	7
Confidentiality of medical data	*Confidentiality of medical data*	The system shall ensure that medical data can be accessed by authorized users only.	1
Control of access rights to medical data by patients	*Control of access rights to medical data by patients* including *Ownership of medical data*	The system shall ensure that patients can grant access rights to their medical data by themselves.	3
Revocation of access rights to medical data	*Revocation of access rights to medical data*	The system shall ensure that access rights to medical data can be revoked (e.g., for medical workers at the patient's previous place of treatment).	11
Fine-grained access control to medical data	*Fine-grained access control to medical data*	The system shall ensure that medical data items can be accessed by authorized users only.	8
Flexible access to medical data	*Flexible access to medical data*	The system shall ensure that medical data can be accessed in exceptional situations without patients' involvement (e.g., in emergency cases or in case of a legal investigation of malpractices).	5
Integrity of medical data	*Integrity of medical data*	The system shall ensure that medical data can be modified by authorized users only.	4
Availability of medical data	*Availability* including *Robustness* and *Up-to-dateness* and *Long-term storage of medical data* (e.g., through *Archiving and recoverability*)	The system shall ensure that the medical data is always available and up-to-date.	10
Usability, scalability and efficiency of the system	*Usability, scalability and efficiency of the system*	The system shall ensure that it is easy and efficient in use.	6
Control of use and modification of medical data	*Authenticity and authentication of users* and *Non-repudiation* and *Auditability of users' actions* and *Detection and prevention of security attacks and violations*	The system shall ensure that all activities are recorded to detect and prevent illegal actions on time.	2

4.2.2 Ranks and Relative Importance of Security and Privacy Requirements. BWS provides a method to obtain a rank order of requirements in terms of their relative importance. To enable a consistency check of the delivered results, we employ counting analysis, and the square root method. The level of agreement among study participants on the obtained rankings is calculated based on Kendall's coefficient of concordance (Kendall's W). For the numerical and statistical analysis of the survey data, R version 3.5.1 was used.

Table 6. Balanced Incomplete Block Design for 11 Choice Sets and 11 Requirements

Block	Security and privacy requirements				
1	1	2	3	5	8
2	8	9	10	1	4
3	4	5	6	8	11
4	10	11	1	3	6
5	2	3	4	6	9
6	9	10	11	2	5
7	11	1	2	4	7
8	6	7	8	10	2
9	7	8	9	11	3
10	5	6	7	9	1
11	3	4	5	7	10

Table 7. Analysis of Security and Privacy Requirements

Requirement	Most counts	Least counts	Average M-L score	SQRT (M/L + 0.5)	Relative importance	Rank
Confidentiality of medical data	459	44	0.36	3.21	100.00	1
Integrity of medical data	432	47	0.34	3.02	93.90	2
Control of data use and modification	339	102	0.21	1.82	56.63	3
Patients' anonymity	332	193	0.12	1.31	40.79	4
Patients' control of access rights to medical data	261	155	0.09	1.30	40.34	5
Availability of medical data	186	160	0.02	1.08	33.52	6
Fine-grained access control to medical data	195	237	−0.04	0.91	28.21	7
Revocation of access to medical data	135	193	−0.05	0.84	26.01	8
Flexible access to medical data	88	220	−0.12	0.63	19.67	9
Anonymity of medical workers	68	535	−0.41	0.36	11.10	10
Usability, scalability and efficiency of the system	24	633	−0.53	0.19	6.06	11

Ranks based on counting analysis. Counting analysis is executed by first counting the number of times requirements were chosen as the most and the least important (see columns "Most counts" and "Least counts" of Table 7, respectively). As each requirement appeared in five alternative sets in the online survey (see Table 6), the highest value to be received for each single requirement was 1,145 (229 times 5). The results reveal that confidentiality of medical data (459) was most frequently chosen as the most important requirement, whereas usability, scalability and efficiency of the system (28) was mostly regarded as the least important one.

Next, M-L scores are calculated by subtracting the number of times a requirement was identified as the most important from the number of times it was chosen as the least important [Finn and Louviere 1992]. The positive M-L scores of confidentiality (459 − 44 = 415) and integrity (385) of medical data, control of medical data use and modification (237), anonymity of patients (139), control of access rights to medical data through patients (106), and availability of medical data (26) indicate that these requirements were chosen more frequently as most than as least important. The negative M-L scores of usability, scalability and efficiency of the system (−609), anonymity of clinicians (−467), flexible access to medical data (−132), revocation of access rights to medical data (−58) and fine-grained access control to medical data (−42) indicate that these requirements were chosen as the most important less frequently than as the least important.

Table 8. Analysis of Respondent Agreement with Kendall's W

Age group	All	Female	Male
All		0.32^{***}	0.26^{***}
0–20	0.33^{***}	0.34^{***}	0.35^{***}
21–30	0.29^{***}	0.34^{***}	0.24^{***}
31–40	0.32^{***}	0.3^{***}	0.44^{***}
41–50	0.51	0.51	NA
No answer	0.6	0.98	0.97

After that, average M-L scores are calculated for every requirement by dividing the M-L scores by the number of respondents (229) and the number of times every requirement appeared in the choice sets in total (5). These scores allow to create a rank order of requirements, where a higher average M-L score level indicates a higher level of importance [Cohen et al. 2009]. The average M-L scores range from −1 to 1 and provide equivalent results to the M-L scores.

We assign rank 1 to the requirement of the highest importance and rank 11 to the requirement of the lowest importance. At the top of the hierarchy, there are confidentiality of medical data (rank 1), integrity of medical data (rank 2), and control of data use and modification (rank 3). These requirements are followed by patients' anonymity (rank 4), control of access rights to medical data through patients (rank 5), availability of medical data (rank 6), fine-grained access control to medical data (rank 7), and revocation of access rights to medical data (rank 8). The last and the least important requirements involve flexible access to medical data (rank 9), anonymity of medical workers (rank 10), and usability, scalability and efficiency of the system (rank 11).

Relative importances based on the square root method. According to the guidelines by Cohen et al. [2009], the square roots are first taken from the most scores (M) divided by the least (L) scores plus 0.5. The calculated square roots estimate the choice probability of several requirements in percent and are to put in relation to the most important one (with the highest square root) (see Table 7). The most relevant requirement receives a factor of 100 [Cohen et al. 2009; Auger et al. 2007; Flynn et al. 2007; Marley and Louviere 2005]. Column "Relative importance" of Table 7 outlines the relative importances of requirements based on the square root analysis. The detected importances support the findings of the counting analysis.

Level of agreement. We apply Kendall's coefficient of concordance (Kendall's W) on individual M-L scores to examine to what extent respondents agree on the requirement ranking. Kendall's W takes on values between 0 and 1, whereas higher values of Kendall's W indicate higher levels of agreement among the judges [Legendre 2005]. In this study, Kendall's W amounted to 0.29 for the overall sample, 0.32 for female patients and 0.26 for male patients. As for age groups, we received 0.33 for people aged less than 21, 0.29 for people aged between 21 and 30 years old, 0.32 for people aged between 31 and 40 years old, all statistically significant at 0.01 level (see Table 8). For people aged between 41 and 50 and those of unknown age, we received Kendall's W of 0.51 and 0.60, respectively, however, both statistically insignificant.

5 DISCUSSION

5.1 Principal Findings

Despite the growing maturity of the cloud computing literature, ensuring information security and privacy in cloud computing environments is still a frequent topic of scholarly debates when it comes to the protection of sensitive data (e.g., health data) stored in the cloud. Especially the consumers' (i.e., the patients') perspective is still underrepresented in the literature. With this

research, we set out to address this issue by conducting a comprehensive literature review on information security and privacy requirements for healthcare cloud services and subsequently obtaining a ranking of those identified requirements from the patients' perspective.

The comprehensive literature review conducted during the first phase of this study yielded a total of 20 information security and information privacy requirements. As we derived requirements from the literature, we thoroughly defined each requirement and discussed definitions with multiple researchers. Not only did this ensure a clear distinction between individual requirements but also revealed the existence of several interdependencies between the derived requirements. The analysis of the derived requirements highlighted that the results of our literature review are mostly consistent with those by Ermakova et al. [2013a] and are also reflected in the specified process-driven user goals [Natsiavas et al. 2019; Junghanns et al. 2016; Fabian et al. 2015b]. In particular, confidentiality of medical data, ownership of medical data, fine-grained access control to medical data, flexible access control to medical data, revocation of access control to medical data, control of access rights to medical data by patients, patients' anonymity, medical workers' anonymity, unlinkability, integrity of medical data, users' authenticity and authentication, auditability of users' actions, non-repudiation of users' actions, detection and prevention of security attacks and violations, availability of medical data, archiving of medical data, as well as usability, scalability and efficiency of the system are present in our study as well as in the study of Ermakova et al. [2013a]. However, in contrast to previous studies on information security and privacy requirements in healthcare cloud services, confidentiality of medical data existence and users' access rights are considered as part of the unlinkability requirement in this research. Furthermore, instead of availability and utility of the system [Ermakova et al. 2013a] and usability of the system [Natsiavas et al. 2019], we specified more concrete requirements of robustness of the system, long-term storage of medical data, up-to-dateness of medical data, and recoverability of medical data. Although our literature review yielded mostly the same information security and privacy requirements as previous works, cloud computing is a highly dynamic context [Yang and Tate 2012]. It is thus possible that certain information security and privacy requirements change over time or that new information security and privacy requirements will emerge (e.g., due to changes in laws and regulations such as the introduction of the General Data Protection Regulation in the European Union [Parliament and Council 2016]). To see how the results of our literature review compare to recent literature on information security and privacy in healthcare cloud services, we further juxtaposed them to other recent studies in this area. Overall, the present list of information security and information privacy requirements also considers those defined by Dawoud and Altilar [2017], where confidentiality of medical data, flexible access control to medical data, authenticity and authentication (or forgery resistance) of users, anonymity of users, unlinkability (untraceability), detection and prevention of security attacks and violations (DoS and replay attack resist) are addressed. Moreover, our review results also include the requirements suggested by Al-Issa et al. [2019], namely, confidentiality of medical data, ownership of medical data, control of access rights to medical data, anonymity, unlinkability, integrity of medical data, users' authenticity, auditability and non-repudiation of users' actions, availability of medical data, and up-to-dateness of medical data as data remanence and freshness.

Regarding the second phase, we differentiate between requirements that were selected as most important more frequently than as least important and those that were selected as least important more frequently than as most important. In the first group, we see confidentiality (rank 1), integrity of medical data (rank 2), and control of data use and modification (rank 3) at the top of the hierarchy, followed by patients' anonymity (rank 4), patients' control of access rights to medical data (rank 5), and availability of medical data (rank 6). The top ranking of confidentiality substantiates common public perceptions and result of earlier studies. As stated by TRUSTe/NCSA [2016], 9 in

10 U.S. users actually admit worrying about their online privacy and avoiding companies where their privacy is not protected. Accordingly, a series of studies have repeatedly observed privacy concerns as an essential source of attitudes toward online healthcare services [Dinev et al. 2013; Angst and Agarwal 2009], as well as as an impediment to behavioral intentions to use some online healthcare services [Ermakova et al. 2014; Angst and Agarwal 2009] and share medical information for transactions [Bansal and Davenport 2010; Bansal et al. 2010, 2007]. Top-ranked confidentiality of medical data, integrity of medical data, and control of data use and modification constitute responsive measures to reduce the established dimensions of concerns for information privacy such as unauthorized access of information, errors, or collection and unauthorized secondary use of information [Smith et al. 1996]. Anonymity was also shown as being relevant in lowering privacy concerns [Nass et al. 2009] and strengthening the acceptance of sharing health information online [Riordan et al. 2015; Perera et al. 2011; Whiddett et al. 2006]. In addition, Dinev et al. [2013] provide empirical evidence for the importance of the above listed requirement of confidentiality and its enhancements for forming individual's perceptions of control over their personal information. Although perceived benefits of a health cloud scenario can override the impact of privacy concerns [Ermakova et al. 2014], this was apparently not the case for our mainly young and, hence, probably comparatively healthy respondents (rank 6 for availability of medical data). Toward this end, our findings support the observations of Wilkowska and Ziefle [2012] and Lafky and Horan [2011], who argue that healthy individuals attribute higher importance to confidentiality and anonymity than individuals with poor health, and Bellman et al. [2004], who speak about especially private Germans. Among requirements that were chosen as most important less frequently than as least important are fine-grained access control (rank 7), revocation of access to medical data (rank 8), flexible access to medical data (rank 9), medical workers' anonymity (rank 10), as well as usability, scalability and efficiency of the system (rank 11). Although fine-grained access control and revocation of access to medical data can be seen as conceptually closely related to confidentiality of medical data, both requirements were ranked relatively low. Drawing on the privacy paradox [Norberg et al. 2007], we hypothesize that the difference in these requirements' rankings might be a reflection of the discrepancy between stated privacy preferences and actual privacy behavior. As such, patients might, on the one hand, view confidentiality as an abstract yet important good, while, on the other hand, not being disposed to putting high efforts (e.g., managing fine-grained access rights and revoking access) into actually achieving it. We attribute the low rank for flexible access to medical data to the fact that this requirements is related to substantial uncertainties for the participants of this study [Ermakova et al. 2014]. Flexible access to medical data is usually required in situations where patients themselves are unable to grant access to their medical data (e.g., in case of an emergency) [Natsiavas et al. 2019]. Drawing on construal level theory [Trope and Liberman 2010], we argue that such situations are highly abstract for healthy individuals, thus resulting in a relatively low perceived importance. Rank 10 for medical workers' anonymity can be explained by the fact that our study focused on the patients' perspective. Accordingly, we conclude that patients place higher value on their own privacy than on medical professionals' privacy. Although not surprising, this finding highlights the existence of diverse, potentially conflicting perceptions with regard to the importance of information security and information privacy requirements in healthcare cloud services (i.e., medical professionals are likely to place higher emphasis on this requirement). Finally, rank 11 for usability, scalability and efficiency of the system indicates that users place a much higher emphasis on system security and privacy than on practical aspects influencing system implementation and operation; however, users might also be unaware of the implications of higher security for practical operations [Lampson 2009].

Looking at Kendall's W, we see that it is relatively small with a value of approximately 0.29, although statistically significant at the 0.01 level. This indicates that little consensus prevails about

the relative importance of individual requirements among the overall panel. Our estimates of Kendall's W for different patient groups, however, provide empirical support for the existence of different security and privacy views among potential patient end-users of healthcare cloud services. Specifically, we observe values for Kendall's W of 0.33 and 0.26 for female and male patients as well as 0.33, 0.29, and 0.32 for people aged less than 21, between 21 and 30 years old, and between 31 and 40 years old, respectively, all statistically significant at the 0.01 level. For people aged between 41 and 50 and those of unknown age, we received insignificant Kendall's W of 0.51 and 0.60, respectively. However, there were only two people in each of them.

5.2 Implications for Research and Practice

This work has several implications for research and practice. For research, we systematically elicited information security and information privacy requirements in the field of healthcare cloud services and related them to each other in an organized, meaningful way by means of ranking them from the patients' perspective. The need for this was grounded in that the relative importance of information security and information privacy requirements (especially from the patients' perspectives) was largely absent from extant research. Toward this end, our results indicate that the perceived importance of individual requirements is rather heterogeneous among participants and that there might exist different subgroups (e.g., defined by age, sex or health status) within the patients stakeholder group and potentially other stakeholder groups as well. While this warrants further research, our study also shows the feasibility of the BWS method to elicit differences in perceived requirements rankings, as most of the Kendall's W values are significant at the 0.01 level. Since the subjects in our study were primed on a cloud-based scenario at the beginning of the survey, we presume that the obtained requirements ranking is rather cloud-specific. Further, this study differentiated various context-specific, confidentiality-enhancing requirements such as fine-grained access control to medical data, revocation of access control to medical data, control of access rights to medical data by patients, anonymity of patients, anonymity of medical workers, and flexible access to medical data. Nevertheless, we do not rule out a certain degree of generalizability of our findings. Our results might, for instance, be checked for applicability to medical data stored by the medical provider as opposed to a third-party cloud provider. Overall, the requirements framework developed in this research provides a foundation for a further stream of contributions aimed at its extension and refinement (e.g., resolving the issue of interdependencies, investigating rankings of subgroups of stakeholders) over time with further related technological advancements [Yang and Tate 2012] and enriched contexts. It can be applied for prioritization studies using further health-cloud scenarios and from other involved stakeholders' perspectives and provides insights for strengthening security and privacy behavioral research.

From a practical perspective, this study provides essential guidelines for establishing priorities and subsequent implementation releases [Achimugu et al. 2014] and allocating limited resources within the system engineering process to be followed by a health cloud development team. This further suggests what details on security and privacy of medical data should be communicated to patients and to be integrated into the regulations to which health-cloud solutions should comply. The requirements set and ranking procedure can be further developed for supporting crucial decisions on how to improve and evaluate health-cloud solutions in terms of their alignment with patients' intricate security and privacy values [Achimugu et al. 2014].

5.3 Limitations and Future Research

Limitations of this work are as follows. First, although we are confident that our results provide first valuable insights into the relative importance of information security and information privacy requirements in healthcare cloud services from the patients' point of view, consensus

among surveyed patients must be considered relatively weak, as is indicated by the relatively low values for Kendall's W [Schmidt 1997]. Potential sources of the identified variation in participants' opinions were not present in our study design and therefore warrant future research. For example, despite the above-mentioned factors like sex, age, and health status, other privacy-related factors such as awareness about online health technologies [Ancker et al. 2012b; Hwang et al. 2012; Angst et al. 2006], knowledge of privacy invasions [Bansal et al. 2010; Bishop et al. 2005], perceived efficacy of privacy-preserving technological and regulatory mechanisms [Ermakova et al. 2014; Dinev et al. 2012], and trust in third-party cloud computing providers [Ermakova et al. 2014] could be interesting avenues for future research in an attempt to discern how different perceptions of the importance of individual requirements are formed among patients. Adding to this, the requirements engineering process should ideally be executed more than once until the final set of requirements satisfies all involved stakeholders [Sommerville and Sawyer 1997]. To allow for a consistent set of requirements across all stakeholders, multilateral methods such as multilateral security requirements analysis (MSRA) should constitute an integral part of the requirements engineering process [Fabian et al. 2010; Rannenberg et al. 1999]. Owing to its main assumption of multilateral security, MSRA overcomes the drawbacks of traditional analysis methods by presuming that the security and privacy needs of stakeholders are heterogeneous [Fabian et al. 2010]. MSRA has already been adopted as a suitable tool to elicit security and privacy requirements of patients and clinicians and to point out some potential conflicts between them [Ermakova et al. 2013a; TAPAS 2004]. It identifies conflicts and aims at consolidating different security and privacy needs [Fabian et al. 2010; Gürses et al. 2006]. Given the low consensus values in this study, it could also be valuable to explore the application of MSRA to resolve potential conflicts between patient groups if they can be identified more concisely in future work. Furthermore, in line with the multilateral approach of MSRA, similar priority rankings of requirements should be conducted among other stakeholders such as medical workers. Not least, our results provide first indicators that confidentiality requirements such as anonymity for one particular stakeholder group (medical workers) might not be ranked as important by another group (patients) as confidentiality requirements that affect the group itself. This may indicate a need to better reflect and integrate insights from construal level theory [Trope and Liberman 2010] into MSRA. Future research should address such cross-stakeholder priority rankings in more depth to provide a clearer view on such differences, supporting intra- as well as inter-stakeholder communication and consolidation of requirements.

Second, since less than half of the initially elicited requirements could not be included in the survey, due to limitations of BWS experiment designs, future research needs to find a comprehensive method to prioritize a complete set of requirements or simply rank those requirements that we left out. Potential avenues for this could be Express BWS or Sparse BWS, both of which have been proposed to conduct BWS experiments with a large set of items [Chrzan and Peitz 2019]. Although we assumed there can be no complete independence between requirements, in our study, we have selected 11 requirements for the ranking such that they were as independent as possible from each other [Achimugu et al. 2014; Saaty 1990]. Specifically, we omitted requirements that can be expressed by the remaining ones [Moisiadis 2002; Kritikos and Plexousakis 2009]. Further investigations could be directed at refining the decision-making process regarding the requirements selection.

Third, as most empirical studies, this work relied on a limited sample size and a rather single study population. According to prior empirical studies on potentially related health information privacy concerns, age [King et al. 2011; Laric et al. 2009; Terry et al. 2007; Associates 2007], sex [Wilkowska and Ziefle 2012; Laric et al. 2009; Terry et al. 2007], health status [Wilkowska and Ziefle 2012; Lafky and Horan 2011; Bansal and Davenport 2010; Laric et al. 2009], education [Hwang et al. 2012; King et al. 2011; Associates 2007], employment [King et al. 2011], and origin [King et al. 2011;

Laric et al. 2009; Bishop et al. 2005] might be essential. With 56.33% females and 43.67% males in the sample, we have comparably many males and females. With 80.35% of participants aged between 21 and 30 years old, 10.48% aged less than 21, and 7.42% in the age between 31 and 40, there were mainly young people among our subjects, who could value confidentiality more than individuals with poor health [Ermakova et al. 2014; Wilkowska and Ziefle 2012; Lafky and Horan 2011]. Adding to this, health status, employment, education, and origin were not part of the present study design. Furthermore, due to the fact that our sample largely consisted of young adults recruited via social networks and at the Humboldt University of Berlin, high variations in these characteristics can be assumed to be rather unlikely. Hence, this study focused rather on German online users who are also often especially concerned about their privacy [Bellman et al. 2004]. It should be one of the future challenges to verify the findings of this study based on a more representative sample.

Finally, another limitation of this study pertains to the provided scenario. Users' security and privacy requirements were derived with respect to a single, simple cloud-based data sharing scenario. Yet, Dehling and Sunyaev [2014] and Natsiavas et al. [2019] studied different cloud-based healthcare applications and how these may induce different security and privacy needs of end-users. It is therefore particularly interesting to investigate how requirements and priorities may change depending on different use cases [Griebel et al. 2015; Sultan 2014b, 2014a; Hsieh et al. 2013; Ahuja et al. 2012; Kuo 2011] in future research [Jarke and Lyytinen 2015]. In light of the expected growth of possible cloud-based healthcare solutions, as well as the rising globalization of cloud computing in healthcare [Weng et al. 2016; Haskew et al. 2015; Lin et al. 2014a; Nagarajan and Sukanesh 2012], it appears to be worthwhile to replicate and explore the results of the present work under other situations described in detail and adjusted to specific real-world conditions, and with different populations from other countries. To this end, the BWS method applied in this study can be easily adapted to different scenarios and be employed for cross-cultural studies, as translation problems of verbal scales to different languages as well as problems that are typical for numerical scales (e.g., different meanings of numbers in different cultures) can be avoided [Lee et al. 2007; Roy et al. 2001].

In spite of the above limitations, we are confident that our work makes valuable contributions to research and practice, which provide a fruitful ground for various avenues of future research on information security and information privacy in healthcare cloud services and their relative importance.

6 CONCLUSION

The wide adoption of cloud computing in healthcare is still hampered by ongoing privacy and security concerns of its potential users. To enhance a wider acceptance and adoption of cloud-based healthcare services, in this study, we examined the security and privacy requirements discussed in the literature and their relative relevance from the perspective of potential patients.

Our results demonstrate that protection of medical data from unauthorized disclosure and modification is of the highest importance to patients. Next, patients strive for the possibility to stay anonymous and control access rights to their medical data in the system. Unauthorized disclosure prevented within medical data and in a later time period, and access to medical data enabled under exceptional conditions form the middle of their ranking. When weighing security and privacy against system usability, scalability and efficiency, patients accept no compromises.

This study can support system developers in designing health-cloud solutions that satisfy the most highly prioritized security and privacy needs of this user group. The results can further fasten the comprehensive negotiation process between the requirements engineers and end users. Further research should attempt to increase the participation rate in the process of requirements

prioritization and involve other stakeholders. Additionally, the requirements engineering process could be applied to further and more concrete cloud-based healthcare solutions. To better account for interacting requirements, the multilateral security requirements analysis should be applied as an important part of the requirements engineering process.

APPENDIX

Table 9. Online Survey Requirement Inclusion

Included requirement	Reason for inclusion
Anonymity of patients	This requirement is included to reflect the sensitive health-related context. Patients should not be identifiable in health data by unauthorized parties.
Anonymity of medical workers	This requirement is included to reflect multilateral security: Not only patients but also medical workers may have (potential) anonymity requirements in health-data processing systems.
Availability of medical data	Availability is an essential requirement of the widely established CIA triad of security engineering.
Confidentiality of medical data	Confidentiality is an essential requirement of the widely established CIA triad of security engineering.
Control of access rights to medical data by patients	Control of access rights to medical data by patients is a fundamental measure to enhance confidentiality of patients' health data according to their own preferences.
Control of use and modification of medical data	Control of use and modification of medical data is an important measure to protect confidentiality and integrity of the data, and to detect misuse. It subsumes the requirements of authenticity and authentication of users, non-repudiation of users' action, auditability of users' actions, and detection and prevention of security attacks and violations.
Fine-grained access control to medical data	Fine-grained access control to medical data (e.g., based on roles as in RBAC) leads to a better reflection of the "need-to-know" principle as well as to enhanced confidentiality and integrity.
Flexible access to medical data	Flexible access to medical data (e.g., in emergencies without patients' involvement or to provide more efficient healthcare processes) results in important trade-offs with other security requirements.
Integrity of medical data	Integrity is an essential requirement of the widely established CIA triad of security engineering.
Revocation of access rights to medical data	Revocation of access rights could improve long-term confidentiality and integrity by reducing the number of authorized persons that can access the data.
Usability, scalability and efficiency of the system	System usability, scalability and efficiency could result in potential conflicts with the other included requirements. Such trade-offs are common results of security engineering decisions and system implementations.

Table 10. Online Survey Requirement Exclusion

Excluded requirement	Dependency	Reasoning
Unlinkability	Anonymity of patients and medical workers	Unlinkability might be difficult to clearly differentiate for some of our study's participants. It is semantically connected to preventing unauthorized monitoring of patients or medical workers across different "observations" or data entries. Anonymity, considered as an "intuitive" concept among study participants, seems to capture the specifics of unlinkability quite well.
	Anonymity of medical workers	
Ownership of medical data	Control of access rights to medical data by patients	Under the legislative frameworks, patients' right to personal medical data protection overrides the property right notion. Data ownership might be a difficult-to-grasp concept and could also refer to different legal connotations among different study participants. Study participants might also become confused and wonder why there could be situations in which they do not own their data. Furthermore, controlling access rights is more concrete and indirectly involves a concept of ownership.
Robustness of the system	Availability of medical data	Availability in general includes availability despite system failures, which is a central goal of robustness.
Up-to-dateness of medical data	Availability of medical data	Availability can also be understood as implicitly referring to "fresh" and recent data, in contrast to outdated data that may be less useful.
Long-term storage of medical data	Availability of medical data	Long-term storage is a measure for availability in general, but it is only indirectly relevant for patients (in contrast to system engineers) and therefore subsumed under availability in our study.
Archiving and recoverability of medical data	Availability of medical data	Archiving and recoverability is a more technical requirement from system engineering that has the goal of long-term availability. Moreover, healthcare providers can be obliged to keep medical files for an established long-term retention period or even permanently, what would require them to move medical data no longer actively used to a separate storage device or archive. As such, it is only indirectly relevant for patients and is in our study subsumed under availability.
Authenticity and authentication of users	Control of use and modification of medical data	Authenticity and authentication of users are a priori requirements for control and use of modification that are geared towards system engineering. Their general goal is to support the prevention of the unauthorized access and modification of medical data. From a user perspective, control of use and modification of medical data can therefore be considered as the overarching goal of these requirements.
Non-repudiation of users' action	Control of use and modification of medical data	Non-repudiation (e.g., of actions such as accessing and modifying patient data) is, from a user's perspective, part of the control of use and modification of medical data as it is semantically connected to the concept of control. Furthermore, the term might be unfamiliar to a general audience.
Auditability of users' actions	Control of use and modification of medical data	Auditability can be seen as a more operational perspective on non-repudiation and therefore also part of the control of use and modification of medical data. The term could also refer to different legal connotations among different study participants.
Detection and prevention of security attacks and violations	Control of use and modification of medical data	Detection and prevention of security attacks and violations is a more technical requirement from systems (security) engineering, which has the ultimate goal of preventing unauthorized access and use of systems and data. From a patient's perspective, it can therefore be regarded as part of the control of use and modification of medical data.

REFERENCES

Imad M. Abbadi, Mina Deng, Marco Nalin, Andrew Martin, Milan Petkovic, Ilaria Baroni, and Alberto Sanna. 2011. Trustworthy middleware services in the cloud. In *Proceedings of the 3rd ACM International Workshop on Cloud Data Management*. 33–40.

Assad Abbas and Samee U. Khan. 2014. A review on the state-of-the-art privacy preserving approaches in the e-health clouds. *IEEE J. Biomed. Health Inform.* 18, 4 (2014), 1431–1441.

Philip Achimugu, Ali Selamat, Roliana Ibrahim, and Mohd Naz'ri Mahrin. 2014. A systematic literature review of software requirements prioritization research. *Info. Softw. Technol.* 56, 6 (2014), 568–585.

Sanjay P. Ahuja, Sindhu Mani, and Jesus Zambrano. 2012. A survey of the state of cloud computing in healthcare. *Netw. Commun. Technol.* 1, 2 (2012), 12–19.

Yazan Al-Issa, Mohammad Ashraf Ottom, and Ahmed Tamrawi. 2019. eHealth cloud security challenges: A survey. *J. Healthcare Eng.* 2019, 1 (Sep. 2019), 1–15.

Jessica S. Ancker, Alison M. Edwards, Melissa C. Miller, and Rainu Kaushal. 2012a. Consumer perceptions of electronic health information exchange. *American J. Prevent. Med.* 34, 1 (2012), 76–80.

Jessica S. Ancker, Michael Silver, Melissa C. Miller, and Rainu Kaushal. 2012b. Consumer experience with and attitudes toward health information technology: A nationwide survey. *Amer. Med. Inform. Assoc.* 20, 1 (2012), 152–156.

Catherine L. Anderson and Ritu Agarwal. 2011. The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Info. Syst. Res.* 22, 3 (2011), 469–490.

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

Corey M. Angst and Ritu Agarwal. 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quart.* 2, 33 (2009), 339–370.

Corey M. Angst, Ritu Agarwal, and Janelle Downing. 2006. An empirical examination of the importance of defining PHR for research and for practice. *Robert H. Smith School Research Paper No. RHS-06-011* (2006).

Radha Appan and Glenn J. Browne. 2012. The impact of analyst-induced misinformation on the requirements elicitation process. *MIS Quart.* 36, 1 (2012), 85–106.

Ajit Appari and M. Eric Johnson. 2010. Information security and privacy in healthcare: Current state of research. *Int. J. Internet Enterprise Manage.* 6, 4 (2010), 279–314.

EKOS Research Associates. 2007. *Electronic Health Information and Privacy Survey: What Canadians Think—2007.* Technical Report. EKOS. Retrieved from https://www.infoway-inforoute.ca/en/component/edocman/resources/reports/privacy/14-ekos-survey-on-electronic-health-information-and-privacy-full.

Giuseppe Ateniese, Reza Curtmola, Breno De Medeiros, and Darren Davis. 2003. Medical information privacy assurance: Cryptographic and system aspects. In *Security in Communication Networks.* Springer, 199–218.

Pat Auger, Timothy M. Devinney, and Jordan J. Louviere. 2007. Using best–worst scaling methodology to investigate consumer ethical beliefs across countries. *J. Bus. Ethics* 70, 3 (2007), 299–326.

Aman Banerjee, Brenda Zosa, Debra Allen, Patricia A. Wilczewski, Robert Ferguson, and Jeffrey A. Claridge. 2016. Implementation of an image sharing system significantly reduced repeat computed tomographic imaging in a regional trauma system. *J. Trauma Acute Care Surg.* 80, 1 (2016), 51–4.

Gaurav Bansal and Rebecca Davenport. 2010. Moderating role of perceived health status on privacy concern factors and intentions to transact with high versus low trustworthy health website. In *Proceedings of the 5th Midwest Association for Information Conference (MWAIS'10).*

Gaurav Bansal and Fatemeh "Mariam" Zahedi. 2010. Trading trust for discount: Does frugality moderate the impact of privacy and security concerns? In *Proceedings of the 16th Americas Conference on Information Systems (AMCIS'10).*

Gaurav Bansal, Fatemeh "Mariam" Zahedi, and David Gefen. 2007. The impact of personal dispositions on privacy and trust in disclosing health information online. In *Proceedings of the 13th Americas Conference on Information Systems (AMCIS'07).*

Gaurav Bansal, Fatemeh "Miriam" Zahedi, and David Gefen. 2008. Efficacy of privacy assurance mechanisms in the context of disclosing health information online. In *Proceedings of the 14th Americas Conference on Information Systems (AMCIS'08).*

Gaurav Bansal, Fatemeh "Mariam" Zahedi, and David Gefen. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information. *Online Decis. Supp. Syst.* 49, 2 (2010), 138–150.

Johannes Barnickel, Hakan Karahan, and Ulrike Meyer. 2010. Security and privacy for mobile electronic health monitoring and recording systems. In *Proceedings of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks.* 1–6.

Randolph C. Barrows and Paul D. Clayton. 1996. Privacy, confidentiality, and electronic medical records. *J. Amer. Med. Inform. Assoc.* 3, 2 (1996), 139–148.

Sujoy Basu, Alan Karp, Jun Li, Jim Pruyne, Jerry Rolia, Sharad Singhal, Jaap Suermondt, and Ram Swaminathan. 2012. Fusion: Managing healthcare records at cloud scale. *Computer* 45, 11 (Nov. 2012), 42–49.

Hans Baumgartner and Jan-Benedict E. M. Steenkamp. 2001. Response styles in marketing research: A cross-national investigation. *J. Market. Res.* 38, 2 (2001), 143–156.

Md. Rizwan Beg, Qamar Abbas, and Ravi Prakash Verma. 2008. Interview process model for requirement elicitation. *Int. J. Comput. Sci. Appl.* 1, 2 (2008), 109–113.

Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. International differences in information privacy concerns: A global survey of consumers. *Info. Soc.* 20, 5 (2004), 313–324.

Alexander Benlian, William Kettinger, Ali Sunyaev, and Till J. Winkler. 2018. The transformative value of cloud computing: A decoupling, platformization, and recombination theoretical framework. *J. Manage. Info. Syst.* 35, 3 (2018), 719–739.

Lynne "Sam" Bishop, Bradford J. Holmes, and Christopher M. Kelley. 2005. *National Consumer Health Privacy Survey 2005*. Technical Report. Forrester Research, Inc. Retrieved from http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005.

Corentin Burnay. 2016. Are stakeholders the only source of information for requirements engineers? Toward a taxonomy of elicitation information sources. *ACM Trans. Manage. Info. Syst.* 7, 3 (2016).

Carole Cadwalladr and Emma Graham-Harrison. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Lingfeng Chen and Doan B. Hoang. 2011. Novel data protection model in healthcare cloud. In *Proceedings of the 13th International Conference on High Performance Computing and Communications*. 550–555.

Tzer-Shyong Chen, Chia-Hui Liu, Tzer-Long Chen, Chin-Sheng Chen, Jian-Guo Bau, and Tzu-Ching Lin. 2012a. Secure dynamic access control scheme of PHR in cloud computing.*J. Med. Syst.* 36, 6 (2012), 4005–4020.

Yu-Yi Chen, Jun-Chao Lu, and Jinn-Ke Jan. 2012b. A secure EHR system based on hybrid clouds. *J. Med. Syst.* 36, 5 (2012), 3375–3384.

Keith Chrzan and Megan Peitz. 2019. Best-worst scaling with many items. *J. Choice Model.* 30, 2019 (2019), 61–72.

William G. Cochran and Gertrude M. Cox. 1957. *Experimental Designs* (2nd ed.). John Wiley & Sons, New York.

Eli Cohen, Steve Goodman, and Eli Cohen. 2009. Applying best-worst scaling to wine marketing. *Int. J. Wine Bus. Res.* 21, 1 (2009), 8–23.

Steve Cohen. 2003. Maximum difference scaling: Improved measures of importance and preference for segmentation. In *Proceedings of the Sawtooth Software Conference*. 61–74.

Steven H. Cohen and Paul Markowitz. 2002. Renewing market segmentation: Some new tools to correct old problems. In *Proceedings of the ESOMAR Congress*. 595–612.

Steven H. Cohen and Leopoldo Neira. 2003. Measuring preference for product benefits across countries: Overcoming scale usage bias with maximum difference scaling. In *Proceedings of the ESOMAR Latin America Conference*.

Bill Davey and Kevin R. Parker. 2015. Requirements elicitation problems: A literature analysis. *IssuesInform. Sci. Info. Technol.* 12 (2015), 71–82.

Mohanad Dawoud and D. Turgay Altilar. 2017. Cloud-based e-health systems: Security and privacy challenges and solutions. In *Proceedings of the 2nd IEEE International Conference on Computer Science and Engineering*.

Bart De Decker, Mohamed Layouni, Hans Vangheluwe, and Kristof Verslype. 2008. A privacy-preserving eHealth protocol compliant with the belgian healthcare system. In *Public Key Infrastructure*. Springer, 118–133.

Tobias Dehling and Ali Sunyaev. 2014. Secure provision of patient-centered health information technology services in public networks—Leveraging security and privacy features provided by the German nationwide health information technology infrastructure. *Electronic Markets* 24, 2 (2014), 89–99.

Mina Deng, Marco Nalin, Milan Petković, Ilaria Baroni, and Abitabile Marco. 2012. Towards trustworthy health platform cloud. In *Proceedings of the 9th VLDB Workshop*. Springer, 162–175.

Mina Deng, Milan Petkovic, Marco Nalin, and Ilaria Baroni. 2011. A home healthcare system in the cloud—Addressing security and privacy challenges. In *Proceedings of the IEEE International Conference on Cloud Computing*. 549–556.

Tamara Dinev, Valentina Albano, Heng Xu, Alessandro D'Atri, and Paul Hart. 2012. Individual's attitudes towards electronic health records—A privacy calculus perspective. *Ann. Info. Syst.* 19 (2012), 19–50.

Tamara Dinev, Heng Xu, Jeff H. Smith, and Paul Hart. 2013. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European J. Info. Syst.* 22 (2013), 295–316.

Saeede Eftekhari, Niam Yaraghi, Ranjit Singh, Ram Danturti Gopal, and Ram Ramesh. 2017. Do health information exchanges deter repetition of medical services? *ACM Trans. Manage. Info. Syst.* 8, 1 (2017).

Tatiana Ermakova, Benjamin Fabian, and Rüdiger Zarnekow. 2013a. Security and privacy system requirements for adopting cloud computing in healthcare data sharing scenarios. In *Proceedings of the 19th Americas Conference on Information Systems*. 1–8.

Tatiana Ermakova, Benjamin Fabian, and Rüdiger Zarnekow. 2014. Acceptance of health clouds—A privacy calculus perspective. In *Proceedings of the 22nd European Conference on Information Systems (ECIS'14)*.

Tatiana Ermakova, Benjamin Fabian, and Rüdiger Zarnekow. 2016. Improving individual acceptance of health clouds through confidentiality assurance. *J. Appl. Clin. Inform.* 7, 4 (2016), 983–993.

Tatiana Ermakova, Jan Huenges, Koray Erek, and Rüdiger Zarnekow. 2013b. Cloud computing in healthcare—A literature review on current state of research. In *Proceedings of the 19th Americas Conference on Information Systems (AMCIS'13)*. 1–8.

Benjamin Fabian, Annika Baumann, and Jessika Lackner. 2015a. Topological analysis of cloud service connectivity. *Comput. Industr. Eng.* 88 (Oct. 2015), 151–165.

Benjamin Fabian, Tatiana Ermakova, and Philipp Junghanns. 2015b. Collaborative and secure sharing of healthcare data in multi-clouds. *Info. Syst.* 48, March 2015 (March 2015), 132–150.

Benjamin Fabian, Seda Gürses, Maritta Heisel, Thomas Santen, and Holger Schmidt. 2010. A comparison of security requirements engineering methods. *Require. Eng.* 15, 1 (2010), 7–40.

FFIEC. 2008. *Authentication in an Internet Banking Environment.* Technical Report. Federal Financial Institutions Examination Council.

Adam Finn and Jordan J. Louviere. 1992. Determining the appropriate response to evidence of public concern: The case of food safety. *J. Public Policy Market.* 11, 2 (1992), 12–25.

Donald Firesmith. 2004. Prioritizing requirements. *J. Object Technol.* 3, 8 (2004), 35–48.

Terry N. Flynn, Jordan J. Louviere, Tim J. Peters, and Joanna Coast. 2007. Best–worst scaling: What it can do for health care research and how to do it. *J. Health Econ.* 26, 1 (2007), 171–189.

Hideo Fujita, Yuji Uchimura, Kayo Waki, Koji Omae, Ichiro Takeuchi, and Kazuhiko Ohe. 2013. Development and clinical study of mobile 12-lead electrocardiography based on cloud computing for cardiac emergency. *Studies Health Technol. Inform.* 192, 1 (Aug. 2013), 1077–1077.

Fangjian Gao and Ali Sunyaev. 2019. Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. *Int. J. Info. Manage.* 48 (2019), 120–138.

Fangjian Gao, Scott Thiebes, and Ali Sunyaev. 2016. Exploring cloudy collaboration in healthcare: An evaluation framework of cloud computing services for hospitals. In *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS'16).* 979–988.

Fangjian Gao, Scott Thiebes, and Ali Sunyaev. 2018. Rethinking the meaning of cloud computing for healthcare: A taxonomic perspective and future research directions. *J. Med. Internet Res.* 20, 7 (2018), e10041.

Margaret Gerteis. 1993. *Through the Patient's Eyes: Understanding and Promoting Patient-Centered Care.* Jossey-Bass, San Francisco.

Ali Gholami, Anna-Sara Lind, Jane Reichel, Jan-Eric Litton, Ake Edlund, and Erwin Laure. 2014. Privacy threat modeling for emerging BiobankClouds. *Procedia Comput. Sci.* 37 (2014), 489–496.

Lena Griebel, Hans-Ulrich Prokosch, Felix Köpcke, Dennis Toddenroth, Jan Christoph, Ines Leb, Igor Engel, and Martin Sedlmayr. 2015. A scoping review of cloud computing in healthcare. *MC Med. Inform. Decis. Mak.* 15, 1 (2015).

Seda Gürses, Bettina Berendt, and Thomas Santen. 2006. Multilateral security requirements analysis for preserving privacy in ubiquitous environments. In *Proceedings of the UKDU Workshop.* 51–64.

Seda Gürses, Jens H. Jahnke, Christina Obry, Adeniyi Onabajo, Thomas Santen, and Morgan Price. 2005. Eliciting confidentiality requirements in practice. In *Proceedings of the 15th Annual International Conference hosted by the IBM Centers for Advanced Studies.* 101–116.

Seda Gürses and Thomas Santen. 2006. Contextualizing security goals: A method for multilateral security requirements elicitation. In *Sicherheit*, Vol. 6. 42–53.

John Haskew, Gunnar Rø, Kaori Saito, Kenrick Turner, George Odhiambo, Annah Wamae, Shahnaaz Sharif, and Tomohiko Sugishita. 2015. Implementation of a cloud-based electronic medical record for maternal and child health in rural Kenya. *Int. J. Med. Inform.* 84, 5 (2015), 349–354.

HHS. 2000. *Summary of the HIPAA Privacy Rule.* Technical Report. United States Department of Health & Human Services. Retrieved from https://www.hhs.gov/sites/default/files/privacysummary.pdf.

Jui-Chien Hsieh, Ai-Hsien Li, and Chung-Chi Yang. 2013. Mobile, cloud, and big data computing: Contributions, challenges, and new directions in telecardiology. *Int. J. Environ. Res. Public Health* 10, 11 (2013), 6131–53.

Jie Huang, Mohamed Sharaf, and Chin-Tser Huang. 2012. A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud. In *Proceedings of the 41st International Conference on Parallel Processing Workshops.* 279–287.

Hsin-Ginn Hwang, Hwai-En Han, Kuang-Ming Kuo, and Chung-Feng Liu. 2012. The differing privacy concerns regarding exchanging electronic medical records of Internet users in Taiwan. *J. Med. Syst.* 36, 6 (2012), 3783–3793.

IEEE. 1990. *IEEE Standard Glossary of Software Engineering Terminology.* Technical Report. C/S2ESC—Software & Systems Engineering Standards Committee.

Iulia Ion, Niharika Sachdeva, Ponnurangam Kumaraguru, and Srdjan Čapkun. 2011. Home is safer than the cloud! Privacy concerns for consumer cloud storage. In *Proceedings of the 7th Symposium on Usable Privacy and Security.*

Jennifer Israelson and Ebru Celikel Cankaya. 2012. A hybrid web based personal health record system shielded with comprehensive security. In *Proceedings of the 45th Hawaii International Conference on System Science.* 2958–2968.

Matthais Jarke and Kalle J. Lyytinen. 2015. Editorial: "Complexity of systems evolution: Requirements engineering perspective." *ACM Trans. Manage. Info. Syst.* 5, 3 (2015).

Philipp Junghanns, Benjamin Fabian, and Tatiana Ermakova. 2016. Engineering of secure multi-cloud storage. *Comput. Industry* 83 (Dec. 2016), 108–120.

Hao-Yun Kao, Wen-Hsiung Wu, Tyng-Yeu Liang, King-The Lee, Ming-Feng Hou, and Hon-Yi Shi. 2015. Cloud-based service information system for evaluating quality of life after breast cancer surgery. *PLoS ONE* 10, 9 (2015), e0139252.

Argyro P. Karanasiou and Emile Douilhet. 2016. Never mind the data: The legal quest over control of information & the networked self. In *Proceedings of the IEEE International Conference on Cloud Engineering Workshop (IC2EW'16)*.

Joachim Karlsson. 1996. Software requirements prioritizing. In *Proceedings of the 2nd International Conference on Requirements Engineering*. 110–116.

Tatiana King, Ljiljana Brankovic, and Patricia Gillard. 2011. Perspectives of Australian adults about protecting the privacy of their health information in statistical databases. *J. Med. Inform.* 81 (2011), 279–289.

Kyriakos Kritikos and Dimitris Plexousakis. 2009. Mixed-integer programming for QoS-based web service matchmaking. *IEEE Trans. Services Comput.* 2, 2 (2009), 122–139.

Raoul Kübler. 2012. Essays on corporate communication: Empirical applications to product recall communication and advertising creativity. *PhD Dissertation, University of Kiel, Faculty of Business, Economics and Social Sciences*.

K. M. Kuo, C. C. Ma, and J. W. Alexander. 2013. How do patients respond to violation of their information privacy. *Health Info. Manage. J.* 43, 2 (2013), 23–33.

Mu-Hsing Kuo. 2011. Opportunities and challenges of cloud computing to improve health care services. *J. Med. Internet Res.* 13, 3 (2011), e67.

Deborah Beranek Lafky and Thomas A. Horan. 2011. Personal health records: Consumer attitudes toward privacy and security of their personal health information. *Health Inform. J.* 17, 1 (2011), 63–71.

Butler Lampson. 2009. Privacy and security Usable security: How to get it. *Commun. ACM* 52, 11 (2009), 25–27.

Jens Lansing, Stephan Schneider, and Ali Sunyaev. 2013. Cloud service certifications: Measuring consumers' preferences for assurances. In *Proceedings of the 21st European Conference on Information Systems (ECIS'13)*. 1–12.

Michael V. Laric, Dennis A. Pitta, and Lea Prevel Katsanis. 2009. Consumer concerns for healthcare information privacy: A comparison of US and Canadian perspectives. *Res. Healthcare Financial Manage.* 12, 1 (2009), 93–111.

Rabia Latif, Haider Abbas, and Saïd Assar. 2014. Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: A systematic literature review. *J. Med. Syst.* 38, 11 (2014), 128.

Julie Anne Lee, Geoffrey N. Soutar, and Jordan Louviere. 2007. Measuring values using best-worst scaling: The LOV example. *Psychol. Market.* 24, 12 (2007), 1043–1058.

Pierre Legendre. 2005. Species associations: The kendall coefficient of concordance revisited. *J. Agric. Biol. Environ. Stat.* 10, 2 (2005), 226–245.

Yair Levy and Timothy J. Ellis. 2006. A systems approach to conduct an effective literature review in support of information systems research. *Inform. Sci. J.* 9 (2006), 181–212.

Ming Li, Shucheng Yu, Ning Cao, and Wenjing Lou. 2011b. Authorized private keyword search over encrypted personal health records in cloud computing. In *Proceedings of the 31st IEEE International Conference on Distributed Computing Systems*. 383–392.

Ming Li, Shucheng Yu, Kui Ren, and Wenjing Lou. 2010. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *Security and Privacy in Communication Networks*, S. Jajodia and J. Zhou (Eds.). Vol. 50. Springer, 89–106.

Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. 2012. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib. Syst.* 24, 1 (2012), 131–143.

Zhuo-Rong Li, En-Chi Chang, Kuo-Hsuan Huang, and Feipei Lai. 2011a. A secure electronic medical record sharing mechanism in the cloud computing platform. In *Proceedings of the IEEE 15th International Symposium on Consumer Electronics*. 98–103.

Angela Lin and Nan-Chou Chen. 2012. Cloud computing as an innovation: Perception, attitude, and adoption. *Int. J. Info. Manage.* 32, 6 (2012), 533–540.

Che-Wei Lin, Shabbir Syed Abdul, Daniel L. Clinciu, Jeremiah Scholl, Xiangdong Jin, Haifei Lu, Steve S. Chen, Usman Iqbal, Maxwell J. Heineck, and Yu-Chuan Li. 2014a. Empowering village doctors and enhancing rural healthcare using cloud computing in a rural area of mainland China. *Comput. Methods Programs Biomed. J.* 113, 2 (2014).

Chia-Yung Lin, Kang-Lin Peng, Ji Chen, Jui-Yuan Tsai, Yu-Chee Tseng, Jhih-Ren Yang, and Min-Huey Chen. 2014b. Improvements in dental care using a new mobile app with cloud services. *J. Formosan Med. Assoc.* 113, 10 (2014), 742–9.

Hans Löhr, Ahmad-Reza Sadeghi, and Marcel Winandy. 2010. Securing the e-health cloud. In *Proceedings of the 1st ACM International Health Informatics Symposium*. 220–229.

James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. 2013. *Disruptive Technologies: Advances That Will Transform Life Business and the Global Economy*. Technical Report. McKinsey Global Institute. Retrieved from http://wwwmckinseycom/insights/business_technology/disruptive_technologies.

Anthony A. J. Marley and Jordan J. Louviere. 2005. Some probabilistic models of best, worst, and best–worst choices. *J. Math. Psychol.* 49, 6 (2005), 464–480.

A. A. J. Marley and T. N. Flynn. 2014. Best worst scaling: Theory and methods. In *Handbook of Choice Modelling*, S. Hess and A. Daly (Eds.). 178–201.

E. J. Melício Monteiro, C. Costa, and J. L. Oliveira. 2016. A cloud architecture for teleradiology-as-a-service. *Methods Info. Med.* 53, 5 (2016), 203–14.

Peter Mell and Timothy Grance. 2011. *The NIST Definition of Cloud Computing*. Technical Report. National Institute of Standards and Technology (NIST). Retrieved from http://csrcnistgov/publications/nistpubs/800-145/SP800-145pdf.

Frank Moisiadis. 2002. The fundamentals of prioritizing requirements. In *Proceedings of Systems Engineering Test and Evaluation Conference*.

Karthikeyan Nagarajan and R. Sukanesh. 2012. Cloud based emergency health care information service in India. *J. Med. Syst.* 36, 6 (2012), 4031–6.

Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin (Eds.). 2009. *Beyond the HIPAA Privacy Rule: Enhancing Privacy. Improving Health Through Research*. National Academies Press, WA.

Pantelis Natsiavas, Christine Kakalou, Konstantinos Votis, Dimitrios Tzovaras, Nicos Maglaveras, and Vassilis Koutkias. 2019. Requirements elicitation for secure and interoperable cross-border health data exchange: The KONFIDO study. *Instit. Eng. Technol.* 13, 3 (2019), 203–210.

Azadeh Nematzadeh and L. Jean Camp. 2010. Threat analysis of online health information system. In *Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments*. 1–7.

Edmund A. M. Neugebauer, Holger Pfaff, Matthias Schrappe, and Gerd Glaeske. 2008. Versorgungsforschung – Konzept, Methoden und Herausforderungen. In *Prävention und Versorgungsforschung: Ausgewählte Beiträge des 2. Nationalen Präventionskongresses und 6. Deutschen Kongresses für Versorgungsforschung, Dresden 24. bis 27. Oktober 2007*.

Patricia A. Norberg, Dan Horne, and David Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. Consumer Affairs* 41, 1 (2007), 100–126.

Ch. Padmini, Sk. Salamuddin, and S. Suresh Babu. 2013. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *Int. J. Recent Innovat. Trends Comput. Commun.* 1, 8 (2013), 679–681.

European Parliament and Council. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from eur-lex.europa.eu.

Gihan Perera, Anne Holbrook, Lehana Thabane, Gary Foster, and Donald J. Willison. 2011. Views on health information sharing and privacy from primary care practices using electronic medical records. *Int. J. Med. Inform.* 80, 2 (2011), 94–101.

John D. Piette, Milton O. Mendoza-Avelares, Martha Ganser, Muhima Mohamed, Nicolle Marinec, and Sheila Krishnan. 2011. A preliminary study of a cloud-computing model for chronic illness self-care support in an underdeveloped country. *American J. Prevent. Med.* 40, 6 (2011), 629–32.

Pascoe Pleasence, Nigel J. Balmer, and Catrina Denvir. 2015. *How People Understand and Interact with the Law*. Technical Report. Legal Education Foundation. Retrieved from https://www.thelegaleducationfoundation.org/wp-content/uploads/2015/12/HPUIL_report.pdf.

Juha Puustjärvi and Leena Puustjärvi. 2013. Practising cloud-based telemedicine in developing countries. *Int. J. Electron. Healthcare* 7, 3 (2013), 181–204.

Kai Rannenberg, Andreas Pfitzmann, and Günther Müller. 1999. IT security and multilateral security. In *Multilateral Security in Communications — Technology, Infrastructure, Economy*, Günther Müller and Kai Rannenberg (Eds.), Vol. 3. Addison-Wesley-Longman, München, 21–29.

Thomas C. Rindfleisch. 1997. Privacy, information technology, and health care. *Commun. ACM* 40, 8 (1997), 92–100.

Laurie A. Rinehart-Thompson. 2008. Storage media profiles and health record retention practice patterns in acute care hospitals. *Perspect. Health Info. Manage.* 5, 9 (2008).

F. Riordan, C. Papoutsi, J. E. Reed, C. Marston, D. Bell, and A. Majeed. 2015. Patient and public attitudes towards informed consent models and levels of awareness of electronic health records in the UK. *Int. J. Med. Inform.* 84, 4 (2015), 237–247.

J. P. C. Rodrigues, I. de la Torre, G. Fernández, and M. López-Coronado. 2013. Analysis of the security and privacy requirements of cloud-based electronic health records systems. *J. Med. Internet Res.* 15, 8 (2013), e186.

Andrew J. Rohm and George R. Milne. 2004. Just what the doctor ordered—The role of information sensitivity and trust in reducing medical information privacy concerns. *J. Bus. Res.* 57, 9 (2004), 1000–1011.

Abhik Roy, Peter G. P. Walters, and Sherriff T. K. Luk. 2001. Chinese puzzles and paradoxes: Conducting business research in China. *J. Bus. Res.* 52, 2 (2001), 203–210.

Chris Rupp. 2005. *UML 2 glasklar: Praxiswissen für die UML-Modellierung und-Zertifizierung*. Carl Hanser Verlag, München.

Thomas L. Saaty. 1990. How to make a decision: The analytic hierarchy process. *European J. Operat. Res.* 48, 1 (1990), 9–26.

John P. Sahlin. 2013. Chapter cloud computing: Past, present, and future. In *Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing*, Xiaoyu Yang and Lu Liu (Eds.). Business Science Reference, 19–50.

Anam Sajid and Haider Abbas. 2016. Data privacy in cloud-assisted healthcare systems: State of the art and future challenges. *J. Med. Syst.* 40, 6 (2016), 155.

Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink, and Charles E. Youman. 1996. Role-based access control models. *IEEE Comput.* 29, 2 (1996).

Roy C. Schmidt. 1997. Managing delphi surveys using nonparametric statistical techniques. *Decision Sci. J.* 28 (1997), 763–774.

S. G. Shini, Tony Thomas, and K. Chithraranjan. 2012. Cloud based medical image exchange-security challenges. *Procedia Eng.* 38 (2012), 3454–3461.

R. Shirey. 2000. *Internet Security Glossary*. Technical Report. The Internet Society. Retrieved from https://www.ietf.org/rfc/rfc2828.txt.

Steven R. Simon, J. Stewart Evans, Alison Benjamin, David Delano, and David W. Bates. 2009. Patients' attitudes toward electronic health information exchange: Qualitative study. *J. Med. Internet Res.* 11, 3 (2009), e30.

H. Jeff Smith, Sandra Milberg, Sandra Milberg, and Sandra J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quart.* 20, 2 (1996), 167–196.

Ian Sommerville and Pete Sawyer. 1997. *Requirements Engineering: A Good Practice Guide*. John Wiley & Sons, Chichester.

Ed Sperling. 2009. Measuring IT security costs. *Forbes* (2009). Retrieved from https://www.forbes.com/2009/02/07/security-information-tech-technology-cio-network_0209_security.html.

William Stallings. 2003. *Cryptography and Network Security: Principles and Practice* (international 3rd ed.). Pearson Education, Upper Saddle River, NJ.

Nabil Sultan. 2014a. Discovering the potential of cloud computing in accelerating the search for curing serious illnesses. *Int. J. Info. Manage.* 34, 2 (2014), 221–225.

Nabil Sultan. 2014b. Making use of cloud computing for healthcare provision: Opportunities and challenges. *Int. J. Info. Manage.* 34, 2 (2014), 177–184.

Ali Sunyaev. 2020. *Cloud Computing*. Springer International Publishing, Cham, 195–236. DOI:https://doi.org/10.1007/978-3-030-34957-8_7

TAPAS. 2004. TAPAS security requirements. Retrieved from http://opentapas.org/.

Amanda L. Terry, Bert M. Chesworth, Paul Stolee, Robert B. Bournee, and Mark Speechley. 2007. Joint replacement recipients' post-surgery views about health information privacy and registry participation. *Health Policy* 85 (2007), 293–304.

Scott Thiebes, Kalle Lyytinen, and Ali Sunyaev. 2017. Sharing is about caring? Motivating and discouraging factors in sharing individual genomic data. In *Proceedings of the 38th International Conference on Information Systems (ICIS'17)*.

Louis L. Thurstone. 1994. A law of comparative judgment. *Psychol. Rev.* 101, 2 (1994), 266–270.

Yaacov Trope and Nira Liberman. 2010. Construal-level theory of psychological distance. *Psychol. Rev.* 117, 2 (2010), 440–463.

TRUSTe/NCSA. 2016. *2016 TRUSTe/NCSA Consumer Privacy Infographic—U.S. Edition*. Technical Report. TRUSTe/NCSA. Retrieved from www.trustarc.com.

Helma van der Linden, Dipak Kalra, Arie Hasman, and Jan Talmon. 2009. Inter-organizational future proof EHR systems: A review of the security and privacy related issues. *Int. J. Med. Inform.* 78, 3 (2009), 141–160.

Jan vom Brocke, Alexander Simons, Bjoern Niehaves, Bjorn Niehaves, Kai Reimer, Ralf Plattfaut, and Anne Cleven. 2009. Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *Proceedings of the 17th European Conference on Information Systems*.

Jan vom Brocke, Alexander Simons, Kai Riemer, Bjoern Niehaves, Ralf Plattfaut, and Anne Cleven. 2015. Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Commun. Assoc. Info. Syst.* 37 (2015), 205–224.

J. Wainer, C. J. R. Campos, M. D. U. Salinas, and D. Sigulem. 2008. Security requirements for a lifelong electronic health record system: An opinion. *Open Med. Inform. J.* 2 (2008), 160–165.

Jane Webster and Richard T. Watson. 2002. Analyzing the past to prepare for the future: Writing a literature review. *MIS Quart.* 26, 2 (2002), 13–23.

Shao-Jen Weng, Donald Gotcher, Hsin-Hung Wu, Yeong-Yuh Xu, Ching-Wen Yang, and Lai-Shiun Lai. 2016. Cloud image data center for healthcare network in Taiwan. *J. Med. Sys.* 40, 4 (2016), 89.

Melinda Whetstone and Ronald Goldsmith. 2009. Factors influencing intention to use personal health records. *Int. J. Pharm. Healthcare Market.* 3, 1 (2009), 8–25.

Richard Whiddett, Inga Hunter, Judith Engelbrecht, and Jocelyn Handy. 2006. Patients' attitudes towards sharing their health information. *Int. J. Med. Inform.* 75, 7 (2006), 530–541.

Wiktoria Wilkowska and Martina Ziefle. 2012. Privacy and data security in e-health: Requirements from the user's perspective. *Health Inform. J.* 18, 3 (2012), 191–201.

Haibo Yang and Mary Tate. 2012. A descriptive literature review and classification of cloud computing research. *Commun. Assoc. Info. Syst.* 31 (2012), 35–60.

Ka-Ping Yee. 2004. Aligning security and usability. *IEEE Secur. Privacy* 2, 5 (2004), 48–55.

Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. 2010. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *Proceedings of the 29th Conference on Information Communications*. 534–542.

Rui Zhang and Ling Liu. 2010. Security models and requirements for healthcare application clouds. In *Proceedings of the 3rd International Conference on Computer Science and Education*. 268–275.

Received February 2017; revised October 2019; accepted February 2020