Improving Individual Acceptance of Health Clouds through Confidentiality Assurance

Tatiana Ermakova[1]; Benjamin Fabian[2]; Rüdiger Zarnekow[3]

[1]Business Informatics, esp. Social Media and Data Science, University of Potsdam, Germany;
[2]Business Intelligence und Data Science, Hochschule fur Telekommunikation Leipzig, Leipzig, Sachsen, Germany;
[3]Department of Information and Communication Management, Technical University of Berlin, Germany

Keywords

Cloud computing, cloud service, cloud storage, data security, privacy, confidentiality, acceptance process

Summary

Background: Cloud computing promises to essentially improve healthcare delivery performance. However, shifting sensitive medical records to third-party cloud providers could create an adoption hurdle because of security and privacy concerns.

Objectives: This study examines the effect of confidentiality assurance in a cloud-computing environment on individuals' willingness to accept the infrastructure for inter-organizational sharing of medical data.

Methods: We empirically investigate our research question by a survey with over 260 full responses. For the setting with a high confidentiality assurance, we base on a recent multi-cloud architecture which provides very high confidentiality assurance through a secret-sharing mechanism: Health information is cryptographically encoded and distributed in a way that no single and no small group of cloud providers is able to decode it.

Results: Our results indicate the importance of confidentiality assurance in individuals' acceptance of health clouds for sensitive medical data. Specifically, this finding holds for a variety of practically relevant circumstances, i.e., in the absence and despite the presence of conventional offline alternatives and along with pseudonymization. On the other hand, we do not find support for the effect of confidentiality assurance in individuals' acceptance of health clouds for non-sensitive medical data. These results could support the process of privacy engineering for health-cloud solutions.

Correspondence to:
Dr. Tatiana Ermakova
August-Bebel-Str. 89
14482 Potsdam, Germany
Email: ermakova@uni-potsdam.de

Appl Clin Inform 2016; 7: 983–993
http://dx.doi.org/10.4338/ACI-2016-07-RA-0107
received: July 3, 2016
accepted: September 12, 016
published: October 26, 2016
Citation: Ermakova T, Fabian B, Zarnekow R. Improving individual acceptance of health clouds through confidentiality assurance. Appl Clin Inform 2016; 7: 983–993
http://dx.doi.org/10.4338/ACI-2016-07-RA-0107
Funding
The work presented in this paper was performed to support the TRESOR research project, which is funded by the German Federal Ministry of Economic Affairs and Energy under grant number 01MD11062.

1.Background and Significance

1.1 Cloud Computing in Healthcare

According to the McKinsey Global Institute's estimates, cloud computing has the potential to affect $3 trillion in worldwide enterprise IT spending [40]. Cloud computing implies a model where virtual machines, development tools and software are provided on demand (e.g., [44]), usually over the Internet [21]. Adopting cloud computing in the medical field can change the face of conventional healthcare delivery [3, 21, 23, 28, 63, 64]. In particular, the technology offers opportunities to resolve several collaborative issues in a diversity of medical services, e.g., by facilitating accessibility of medical data whenever and wherever they are needed [12, 25, 38, 43, 49, 69]. Empirical evidence demonstrates significant improvements related to repetitive medical procedures [12, 20], self-care [26, 47], appointment (re)arrangements and reminders, establishment of a direct doctor-patient relationship [37], and completeness of medical records [22].

Nevertheless, due to involvement of third-party cloud providers, cloud computing still causes serious concerns for many individuals [4, 5, 24, 46, 59] which are related to security and privacy issues [1, 28, 32, 53, 55]. These worries are not unjustified: As a result of the misuse of sensitive medical records, patients might become subject to harassment by healthcare product marketers, discrimination by employers, healthcare insurance agencies and associates, and other threats [8, 10, 31, 54].

1.2Collaborative and Privacy-Enhanced Sharing of Medical Data in Multi-Clouds

Without loss of generality, this paper focuses on so-called health clouds, which provide cloud-based storage services for medical data of healthcare providers [1, 17]. The use of health clouds should involve a patient's informed consent [15]. A variety of approaches have been proposed to preserve the security and privacy of medical data in health clouds [1, 55]. Here, a considerable milestone is the novel *multi-provider cloud architecture* [16, 18], which, as reported by Google Scholar and Researchgate, already enjoyed remarkable publicity.

►Figure 1 gives a high-level overview over this multi-provider cloud architecture. The scenario assumes that there is a patient who visits several different health centers (HCs) successively. At HC A, a medical record (MR) is created. After signing and encrypting (Step 1), the local client software sends it to the local Multi-Cloud Proxy (MCP) (Step 2). The proxy splits the document into shares based on a secret-sharing scheme, and disseminates the shares to different independent Cloud Providers (CP) (Step 3). The procedure used to construct external identifiers for shares enables authorized clients to calculate the identifiers and retrieve the shares. Some time later, the patient visits a second health center, B. Similarly, HC B creates a separate MR which the local client software signs, encrypts (Step 4), and sends to the local MCP (Step 5), where the document is split and distributed in form of shares to different independent CPs (Step 6).

At a third health center, C, a doctor needs the patient's full medical history and requests medical records of HC A and B from the local MCP. After retrieving enough corresponding shares from CPs (Step 7), the local MCP reconstructs the encrypted MRs and sends them to the doctor's local client software (Step 8), where they are decrypted and their authenticity is verified (Step 9).

In an extended version of the architecture, patients can be also monitored by sensor-equipped smart homes, or mobile body-area sensor networks, or smart phones. Mobile medical workers and authorized analysts could be enabled to retrieve data. A private Service Cloud can be used to offer the MCP's cryptographic operations as a service, especially in order to support clients with low-performance hardware.

In comparison to other assurances proposed to preserve privacy in health clouds, the proposed approach guarantees confidentiality of medical records even when encryption keys are compromised or encryption algorithms are broken or insecurely implemented. In this architecture, encrypted health records are divided into different fragments by a secret-sharing scheme such as Shamir's secret-sharing scheme [56]. Shamir defines shares as points of some randomly chosen polynomial and the secret as the y-value of its intersection point with the y-axis. Given less shares than necessary for

the polynomial reconstruction, the intersection point and thus the secret are left undetermined. The document shares are distributed among different cloud services. The secret-sharing mechanism guarantees that a reconstruction of the initial document is only possible in the presence of a certain number of document shares. Therefore, single or small groups of malicious cloud providers are not able to break the confidentiality of health records. These strong confidentiality assurances motivate the use of this novel architecture as a baseline in our current acceptance study.

2. Objectives

Previous research shed light on individuals' security and privacy perceptions of online healthcare information technologies [4, 5, 31, 46, 59, 65, 71, 72]. A series of studies have paid attention to privacy concerns related to the collection and use of healthcare information and shown them to substantially negatively influence attitudes [14, 30], intention [6, 7, 9, 10, 11, 17, 70], and actual behavior [29] regarding online information disclosure, while trust in the privacy-preserving technological mechanisms was found as essential mitigating factor [14, 17]. In the clinical practice, confidentiality assurance could be substantially related to individuals' readiness to share medical data with and seek future health care from physicians [19, 67].

In light of these findings, the present study validates and tightly examines *the effect of confidentiality assurance as a means of increasing acceptance of health clouds among individuals*. Following the previously referred evidence, we postulate the following main research hypothesis:

Research Hypothesis (RH): *Under a high confidentiality assurance, individuals' acceptance of health clouds will increase.*

Additionally, we investigate the main research hypothesis under different conditions such as the sensitivity of medical data and explicate the effect of the presence of conventional offline data-sharing alternatives [15]. These conditions lead to the following subsidiary hypotheses.

RH1: Under a high confidentiality assurance, individuals' acceptance of health clouds for **sensitive medical data** will increase.

RH1a: Under a high confidentiality assurance, individuals' acceptance of health clouds for **sensitive medical data** will increase **despite the presence of conventional offline alternatives.**

RH1b: Under a high confidentiality assurance, individuals' acceptance of health clouds for **sensitive medical data** will increase **in the absence of conventional offline alternatives**.

Researchers argue that removing direct identifiers from medical records does not guarantee their full protection in terms of privacy [27, 42, 35]. Moreover, [35] claim that due to multiple other online data sources, even inaccurate information pieces make people highly identifiable to potential adversaries. Hence, we hypothesize that:

RH1c: *Under a high confidentiality assurance, individuals' acceptance of health clouds* ***for pseudonymized sensitive medical data*** *will increase.*

Finally, we examine the effect of high confidentiality assurance when non-sensitive medical data is shared in the multi cloud, and postulate:

RH2: *Under a high confidentiality assurance, individuals' acceptance of health clouds* ***for non-sensitive medical data*** *will increase.*

3. Methods

3.1Study design

We conducted a survey-based within-subject experimental study. To vary the level of confidentiality assurances, we used two settings, one with low confidentiality assurance and another with high confidentiality assurance. The setting with a stronger assurance of confidentiality was based on the novel multi-provider cloud architecture [16, 18] presented above.

The subjects were asked to *"[i]magine that [their] sensitive patient data could be encrypted and sent from [their] current medical institution to another (a hospital or a doctor) just in the right moment using a cloud-based system*" and rate their intention to give their permission for medical workers to transfer their encrypted sensitive patient data in a cloud-computing environment for seven hypothetical cases on a 7-point Likert scale (answer options: not likely at al, highly unlikely, rather unlikely, neither likely nor unlikely, rather likely, highly likely, fully likely) (▶Table 1).

Next, they were shortly given an idea of how the transfer would work in a high-confidentiality setting:

"*Imagine that your sensitive patient data could be encrypted and sent in single fragments from your current medical institution to another (a hospital or a doctor) just in the right moment using a system based on multiple clouds, where it would be reassembled. Only a relatively large amount of fragments can be used to reassemble your encrypted patient data, otherwise there is absolutely no leakage of information about it. Therefore, no single cloud provider or even small groups of cloud providers can access your encrypted data.*"

Then they were asked the same questions as before. The participants were not shown any other specific information to avoid potential confounding effects. Before starting the study, we validated the survey with multiple individuals of different age, gender and education.

3.2 Data collection

We invited people in Germany and Switzerland to participate in our online study via mailing lists as well as personally and collected responses from November 2013 until January 2014. This focus was adopted because consumers from German and Swiss countries tend to be especially concerned about their privacy [13]. We therefore expected an informed audience in terms of privacy. All participants were informed about our study objectives and were encouraged to learn about cloud computing before taking part in the survey. To make sure that we convey this complex term in an intelligible form [36], we presented its general idea, which we adopted from an established study book on management information systems suitable for introductory undergraduate courses [33, p. 218]. In particular, cloud computing was referred to as the possibility to request software services or data over the Internet.

3.3 Analysis

We analysed the collected data in the R 3.8 statistical computing environment [50]. We applied the paired Student's t-test (e.g., [58, pp. 580–585], [39], [34, p. 100]) and the paired Wilcoxon signed-rank test [39]. Student's t-test was similarly used by Perera et al. [46], Teixeira et al. [65], and Acquisti & Gross [2]. The Wilcoxon signed-rank test was applied by Acquisti & Gross [2].

4. Results

4.1 Demographic data and responses

Two hundred sixty-six of the 464 surveys (57.33%) were fully completed. The participants have mean age of 27.93 years with a standard deviation of 9 years. A slight majority of them are female (53.01%). Five (1.88%) and two (0.75%) respondents did not state their gender and age, respectively. ▶Table 2 provides an overview over responses regarding acceptance of health clouds in the low confidentiality setting and in the high confidentiality setting.

As Table 2 indicates, survey respondents are on average more willing to accept health clouds in the setting with a high confidentiality assurance. Their intentions are closer to the means. Both these observations hold for every considered hypothetical case. Compared to all other cases, survey participants further show lower average acceptance of health clouds in the presence of conventional offline alternatives.

4.2 Results of hypothesis tests

Both Student's t-test and Wilcoxon signed rank test generally confirm that the positive effect of high confidentiality assurance is statistically significant (▶Table 3 for RH1a-c). Only in the least privacy-sensitive base case, i.e., where the sensitive part of patient data was not transmitted (RH2), the increase in individuals' acceptance of health clouds was found not to be significant ($t = 0.39$, $p = 0.35$; $V = 5385$, $p = 0.31$). Regarding pseudonymized medical records (RH1c), the raise in willingness could be confirmed only at a significance level of 5% ($t = 1.83$, $p = 0.03$; $V = 4152$, $p = 0.015$).

5. Discussion

While medical records not timely delivered could result in repeated medical tests and/or delayed medical treatment [17], disclosure of sensitive medical conditions could potentially destroy the individual's social status and employment opportunities [10, 31, 54, 8]. The results of hypothesis testing indicated the importance of high confidentiality in individuals' acceptance of health clouds. Both Student's t-test and Wilcoxon signed rank test confirmed the statistical significance of this effect almost in all considered hypothetical cases (RH1a-c). These results confirm previous findings that individuals prefer to stay anonymous [45, 46, 52, 71] and conceal their sensitive patient data [9, 10, 31, 54, 73] on the Internet.

Only with respect to non-sensitive medical data (RH2), no statistical significance was found in the increase in individuals' acceptance of health clouds. Similarly, researchers argue that confidentiality assured in surveys does not necessary increase respondents' self-disclosure [41, 60, 61], except in case of sensitive questions [61]. Furthermore, empirical evidence observe the links between the type of shared medical data and individuals' attitudes toward their sharing [31, 66, 73] and between perceived sensitivity of shared medical information and individuals' privacy concerns about medical data [9, 10]. This finding is important for further enhancement of the multi-cloud provider architecture and similar future developments: Regarding non-sensitive medical data, weaker confidentiality assurance could be sufficient from the viewpoint of individuals. This would allow for performance trade-offs during systems engineering, such as adopting a more space-efficient alternative instead of Shamir's secret-sharing scheme [51].

In the case of pseudonymization (RH1c), the raise in willingness could be confirmed, though only at a 5% level of significance. Possibly, pseudonymization might slightly have diminished the effect of confidentiality assurance: Prior empirical works actually report on lower privacy concerns [45] and stronger acceptance of health-data sharing in the absence of personal identifiers [46, 52, 71]. As argued by [30], revealing de-identified health information to third parties for purposes of research and business intelligence does not contradict the Health Insurance Portability and Accountability Act (HIPAA).

As in most empirical studies, the sample size used in this study was limited. Many of our subjects were rather young people who are probably more familiar with cloud-computing concepts and may also have experienced relatively few medical problems. For these reasons, it would be interesting to verify the findings of the present research with a more representative sample. On the other hand, some researchers argue that middle-age groups are more concerned about health privacy rather than older and younger age groups [27] and healthy persons attribute higher importance to confidentiality compared to persons with poor health [30, 72]. It further should be noted that this research study was rather focused on examining whether individuals essentially increased their intentions to accept health clouds than describing an overall level of their acceptance.

Furthermore, the focus of this study was laid on German-speaking societies whose citizens often display stronger concerns for privacy [13]. In light of the possible globalization of the investigated application scenario and its introduction into other countries, it would be beneficial to explore the relationships in other cultures. In addition, the cases presented could have appeared somehow hypothetical to the participants. Experimental research with more detailed descriptions of the cases involved could be useful to replicate these study results. However, the cases essentially reflect real situations, which are rather time-critical. Future research may attempt to address these issues.

Following the suggestions by Streiner & Norman [62], we do not correct for multiplicity to avoid type 2 errors as this study is rather aimed to discover fruitful areas of research. We do not control for common method variance (CMV) possible in mono-method research designs [48] due to a strong disagreement in the research community related to this issue [57].

In general, this work considers acceptance of health clouds from the individuals' perspective. Other related aspects worth considering in future work involve laws and more detailed properties of the data.

6. Conclusions

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

Our findings lead to important implications for research and practice. Our paper proposes an evaluation criteria framework to our best knowledge to capture various aspects of inter-organizational sharing of medical data. Healthcare providers wishing to profit from health clouds are provided with a number of possible courses of actions to make them more attractive to their patients. In general, this study shows that individuals' acceptance of health clouds could be strengthened with a stronger confidentiality assurance regarding their sensitive health information. In particular, this can be achieved by cooperating with several independent cloud providers and applying the secret-sharing approach to encrypted medical records before sharing. Moreover, healthcare providers could act as cloud providers themselves. There is no necessity for high confidentiality assurance for non-sensitive medical data, which can be also considered in the engineering of health-cloud solutions.

7. Clinical Relevance Statement

In general, this study demonstrates that individuals' acceptance of health clouds for sensitive medical data could be strengthened with a stronger confidentiality assurance, independent of the presence of conventional offline alternatives and along with pseudonymization. It does not find support for the importance of a high confidentiality assurance regarding non-sensitive medical data.

Conflict of Interest

The authors declare that they have no conflict of interest in the research.

Human Subjects Research Approval

The study was performed in compliance with the World Medical Association Declaration of Helsinki on Ethical Principles of Medical Research Involving Human Subjects.

Acknowledgement

The authors would like to thank for the following contributions to this study: The healthcare experts involved into TRESOR provided valuable insights from the healthcare industry. Dr. Fabian Löser contributed to the design of the online survey. Mr. Jan Huenges contributed to preparing the online survey, and finding and retrieving articles. Ms. Lusine Nazaretyan performed proofreading.

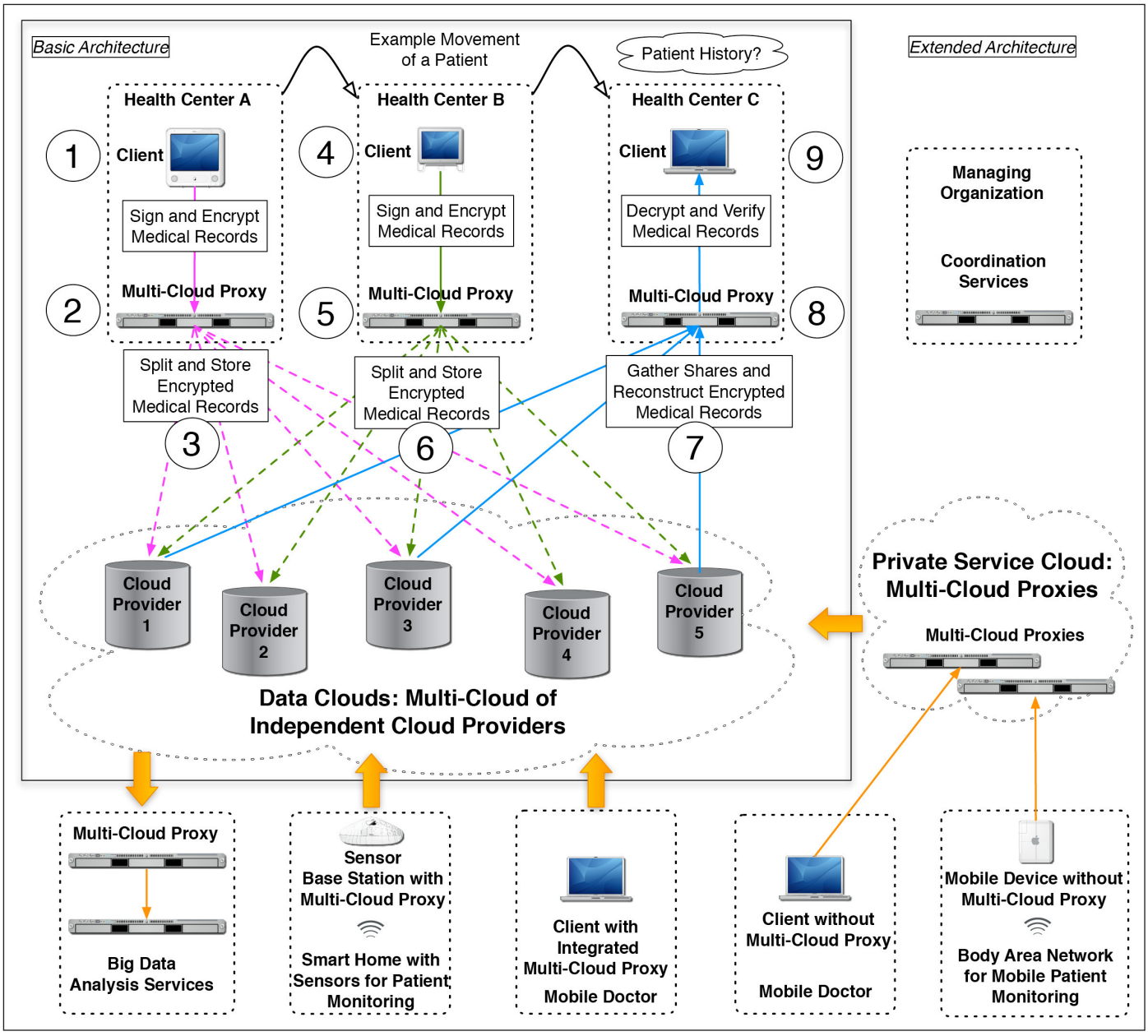

Fig. 1 Architecture overview [18]

Table 1 Research Instrument (based on [17])

RH	Item
	Given the above mentioned circumstances, how likely would you approve to the transmission if …
RH1a	… your patient data could otherwise be transferred via fax.
	… your patient data could otherwise be transferred via taxi.
	… you would have to deal with the transmission yourself.
RH1b	… your patient data could otherwise arrive not in time.
	… it is an emergency situation.
RH1c	… your patient data is pseudonymized (a pseudonym is used instead of your personal identifying data) before being encrypted.
RH2	… the part of your patient data you consider to be sensitive is not transferred.

Table 2 Summary statistics for responses in the low (high) confidentiality setting

Item	Mean	Standard deviation
Acceptance of health clouds if …		
… data could otherwise be transferred via fax. ***(RH1a)***	4.33 (4.93)	2.06 (1.94)
… data could otherwise be transferred via taxi. ***(RH1a)***	4.66 (5.13)	2.11 (1.95)
… data has otherwise to be transferred by individuals. ***(RH1a)***	4.40 (4.86)	2.11 (2.06)
… data could otherwise arrive not in time. ***(RH1b)***	5.23 (5.61)	1.78 (1.58)
… it is an emergency situation. ***(RH1b)***	6.00 (6.18)	1.45 (1.38)
… data is pseudonymized before encryption. ***(RH1c)***	5.52 (5.55)	1.65 (1.74)
… the sensitive part of their data is not transferred. ***(RH2)***	5.38 (5.50)	1.74 (1.73)

Table 3 Results of hypothesis testing

Hypothesis	Student's t-test	Wilcoxon signed rank test
Under a high confidentiality assurance, individuals' acceptance of health clouds …		
*… for **sensitive medical data** will increase **despite the presence of conventional offline alternatives** (i.e., fax). **(RH1a)***	Supported t = 6.76, p < 0.001	Supported V = 8507, p < 0.001
*… for **sensitive medical data** will increase **despite the presence of conventional offline alternatives** (i.e., taxi). **(RH1a)***	Supported t = 5.09, p < 0.001	Supported V = 6528, p < 0.001
*… for **sensitive medical data** will increase **despite the presence of conventional offline alternatives** (i.e., self-transfer). **(RH1a)***	Supported t = 5.35, p < 0.001	Supported V = 6319, p < 0.001
*… for **sensitive medical data** will increase **in the absence of conventional offline alternatives** (timely delivery impossible). **(RH1b)***	Supported t = 4.86, p < 0.001	Supported V = 5360, p < 0.001
*… for **sensitive medical data** will increase **in the absence of conventional offline alternatives** (emergency). **(RH1b)***	Supported t = 2.69, p = 0.004	Supported V = 3018, p < 0.001
*… for **pseudonymized sensitive medical data** will increase. **(RH1c)***	Supported t = 1.83, p = 0.03	Supported V = 4152, p = 0.015
*… for **non-sensitive medical data** will increase. **(RH2)***	Not supported t = 0.39, p = 0.35	Not supported V = 5385, p = 0.31

References

1. Abbas A, Khan SU. A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds. IEEE Journal of Biomedical and Health Informatics 2014; 18(4): 1431–1441.
2. Acquisti A, Gross R. Imagined Communities: Awareness Information Sharing and Privacy on the Facebook. Proceedings of the 6th International Conference Privacy Enhancing Technologies; 2006.
3. Ahuja SP, Mani S, Zambrano J. A Survey of the State of Cloud Computing in Healthcare. Network and Communication Technologies 2012; 1(2): 12–19.
4. Ancker JS, Silver M, Miller MC, Kaushal R. Consumer Experience with and Attitudes toward Health Information Technology: A Nationwide Survey. American Medical Informatics Association 2012; 20(1): 152–156.
5. Ancker JS, Edwards AM, Miller MC, Kaushal R. Consumer Perceptions of Electronic Health Information Exchange. American Journal of Preventive Medicine 2012; 34(1): 76–80.
6. Anderson C, Agarwal R. The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. Information Systems Research 2011; 22(3): 469–490.
7. Angst C, Agarwal R, Downing J. 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.
8. Appari A, Johnson ME. Information Security and Privacy in Healthcare: Current State of Research. International Journal of Internet and Enterprise Management 2010; 6(4): 279–314.
9. Bansal G, Zahedi F, Gefen D. The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online. Proceedings of the 13th Americas Conference on Information Systems (AMCIS); 2007
10. Bansal G, Zahedi F, Gefen D. The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information. Online Decision Support Systems 2010; 49(2): 138–150.
11. Bansal G, Davenport R. Moderating Role of Perceived Health Status on Privacy Concern Factors and Intentions to Transact with High versus Low Trustworthy Health Websites. Proceedings of the 5th MWAIS (Midwest Association for Information) Conference; 2010.
12. Banerjee A, Zosa BM, Allen D, Wilczewski PA, Ferguson R, Claridge JA. Implementation of an Image Sharing System Significantly Reduced Repeat Computed Tomographic Imaging in a Regional Trauma System. Journal of Trauma and Acute Care Surgery 2016; 80 (1): 51–4.
13. Bellman S, Johnson EJ, Kobrin SJ, Lohse GL. International Differences in Information Privacy Concerns: A Global Survey of Consumers. The Information Society 2004; 20(5): 313–324.
14. Dinev T, Albano V, Xu H, D'Atri A, Hart P. Individual's Attitudes Towards Electronic Health Records – A Privacy Calculus Perspective. Annals of Information Systems 2012; 19: 19–50.
15. Dijk A, Busman JP, Van der Putten N, Dassen W. Transmural Exchange of Cardiology Related Information between two Academic Centers and Referring Hospitals Using XDS(-I). Proceedings of the IEEE Conference Computing in Cardiology; 2010.
16. Ermakova T, Fabian B. Secret Sharing for Health Data in Multi-Provider Clouds. Proceedings of the 15th IEEE Conference on Business Informatics (CBI); 2013.
17. Ermakova T, Fabian B, Zarnekow R. Acceptance of Health Clouds – a Privacy Calculus Perspective. Proceedings of the 22nd European Conference on Information Systems (ECIS); 2014.
18. Fabian B, Ermakova T, Junghanns P. Collaborative and Secure Sharing of Healthcare Data in Multi-Clouds. Information Systems 2014; 48: 132–150.
19. Ford CA, Millstein SG, Halpern-Felsher BL, Irwin Jr CE. Influence of Physician Confidentiality Assurances on Adolescents' Willingness to Disclose Information and Seek Future Health Care: A Randomized Controlled Trial. Journal of the American Medical Association 1997; 278(12): 1029–1034.
20. Fujita H, Uchimura Y, Waki K, Omae K, Takeuchi I, Ohe K. Development and Clinical Study of Mobile 12-Lead Electrocardiography Based on Cloud Computing for Cardiac Emergency. Studies in Health Technology and Informatics 2013; 192: 1077.
21. Griebel L, Prokosch HU, Köpcke F, Toddenroth D, Christoph J, Leb I, Engel I, Sedlmayr M. A Scoping Review of Cloud Computing in Healthcare. BMC Medical Informatics and Decision Making 2015; 15(1).
22. Haskew J, Rø G, Saito K, Turner K, Odhiambo G, Wamae A, Sharif S, Sugishita T. Implementation of a Cloud-Based Electronic Medical Record for Maternal and Child Health in Rural Kenya. International Journal of Medical Informatics 2015; 84(5): 349–354.
23. Hsieh JC, Li AH, Yang CC. Mobile, Cloud, and Big Data Computing: Contributions, Challenges, and New Directions in Telecardiology. International Journal of Environmental Research and Public Health 2013; 10(11): 6131–53.

24. Ion I, Sachdeva N, Kumaraguru P, Capkun S. Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage. Proceedings of the 7th Symposium on Usable Privacy and Security; 2011.
25. Karthikeyan N, Sukanesh R. Cloud Based Emergency Health Care Information Service in India. Journal of Medical Systems 2012; 36(6): 4031–4036.
26. Kao HY, Wu WH, Liang TY, Lee KT, Hou MF, Shi HY. Cloud-Based Service Information System for Evaluating Quality of Life after Breast Cancer Surgery. PLoS ONE 2015; 10(9): e0139252.
27. King T, Brankovic L, Gillard P. Perspectives of Australian Adults about Protecting the Privacy of Their Health Information in Statistical Databases. International Journal of Medical Informatics 2012; 81(4): 279–289.
28. Kuo AMH. Opportunities and Challenges of Cloud Computing to Improve Health Care Services. Journal of Medical Internet Research 2011; 13(3): e67.
29. Kuo KM, Ma CC, Alexander J. How do Patients Respond to Violation of their Information Privacy. Health Information Management Journal 2013; 43(2): 23–33.
30. Lafky DB, Horan TA. Personal Health Records: Consumer Attitudes toward Privacy and Security of their Personal Health Information. Health Informatics Journal 2011; 17(1): 63–71.
31. Laric MV, Pitta DA, Katsanis LP. Consumer Concerns for Healthcare Information Privacy: A Comparison of US and Canadian Perspectives. Research in Healthcare Financial Management 2009; 12(1): 93–111.
32. Latif R, Abbas H, Assar S. Distributed Denial of Service (DDoS) Attack in Cloud-Assisted Wireless Body Area Networks: A Systematic Literature Review. Journal of Medical Systems 2014; 38(11): 128.
33. Laudon KC, Laudon JP, Schoder D. Wirtschaftsinformatik – Eine Einführung, 2. aktualisierte Auflage. Pearson Studium; 2010.
34. Li Y, Baron J. Behavioral Research Data Analysis with R. New York: Springer; 2012.
35. Li F, Zou X, Liu P, Chen JY. New Threats to Health Data Privacy. BMC Bioinformatics 2011; 12(12): S7.
36. Lin A, Chen NC. Cloud Computing as an Innovation: Perception, Attitude, and Adoption. International Journal of Information Management 2012; 32(6): 533–540.
37. Lin CY, Peng KL, Chen J, Tsai JY, Tseng YC, Yang JR, Chen MH. Improvements in Dental Care Using a New Mobile App with Cloud Services. Journal of the Formosan Medical Association 2014; 113(10): 742–9.
38. Lin CW, Abdul SS, Clinciu DL, Scholl J, Jin X, Lu H, Chen SS, Iqbal U, Heineck MJ, Li YC. Empowering Village Doctors and Enhancing Rural Healthcare Using Cloud Computing in a Rural Area of Mainland China. Computer Methods and Programs in Biomedicine Journal 2014; 113(2): 585–92.
39. Lowry R. Concepts, Applications of Inferential Statistics; 2013. Available from http://vassarstatsnet/textbook/indexhtml.
40. Manyika J, Chui M, Bughin J, Dobbs R, Bisson P, Marrs A. Disruptive Technologies: Advances That Will Transform Life Business and the Global Economy; 2013. Available from http://wwwmckinseycom/insights/business_technology/disruptive_technologies.
41. McGuire JM; Graves S, Blau B. Depth of Self-Disclosure as a Function of Assured Confidentiality and Videotape Recording. Journal of Counseling & Development 1985; 64(4): 259–263.
42. McGraw D, Dempsey JX, Harris L, Goldman J. Privacy as an Enabler not an Impediment: Building Trust into Health Information Exchange. Health Affairs 2009; 28(2): 416–427.
43. Melício Monteiro EJ, Costa C, Oliveira JL. A Cloud Architecture for Teleradiology-as-a-Service. Methods of Information in Medicine 2016; 55(3): 203–14.
44. Mell P, Grance T. The NIST Definition of Cloud Computing; 2012. Available from http://csrcnistgov/publications/nistpubs/800–145/SP800–145pdf.
45. Nass SJ, Levit LA, Gostin LO. Beyond the HIPAA Privacy Rule: Enhancing Privacy. Improving Health Through Research, Washington: National Academies Press; 2009.
46. Perera G, Holbrook A, Thabane L, Foster G, Willison DJ: Views on Health Information Sharing and Privacy from Primary Care Practices Using Electronic Medical Records. International Journal of Medical Informatics 2011; 80(2): 94–101.
47. Piette JD, Mendoza-Avelares MO, Ganser M, Mohamed M, Marinec N, Krishnan S. A Preliminary Study of a Cloud-Computing Model for Chronic Illness Self-Care Support in an Underdeveloped Country. American Journal of Preventive Medicine 2011; 40(6): 629–32.
48. Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP. Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. Journal of Applied Psychology 2003; 88(5): 879–903.
49. Puustjärvi J, Puustjärvi L. Practising Cloud-Based Telemedicine in Developing Countries. International Journal of Electronic Healthcare 2013; 7(3): 181–204.
50. R Development Core Team. R: A Language and Environment for Statistical Computing R Foundation for Statistical Computing, 2012. Available from http://wwwR-projectorg/.

51. Rabin M. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. Journal of the ACM 1989; 36: 335–348.
52. Riordan F, Papoutsi C, Reed JE, Marston C, Bell D, Majeed A. Patient and Public Attitudes Towards Informed Consent Models and Levels of Awareness of Electronic Health Records in the UK. International Journal of Medical Informatics 2015; 84(4): 237–247.
53. Rodrigues JPC, de la Torre I, Fernández G, López-Coronado M. Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems. Journal of Medical Internet Research 2013; 15(8): e186.
54. Rohm AJ, Milne GR. Just What the Doctor Ordered – The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern. Journal of Business Research 2004; 57(9): 1000–1011.
55. Sajid A, Abbas H. Data Privacy in Cloud-Assisted Healthcare Systems: State of the Art and Future Challenges. Journal of Medical Systems 2016; 40(6): 155.
56. Shamir A. How to Share a Secret. Communications of the ACM 1979; 22(11): 612–613.
57. Sharma R, Yetton P, Crawford J. Estimating the Effect of Common Method Variance: The Method-Method Pair Technique with an Illustration from TAM Research. MIS Quarterly 2009; 33(3): 473–490.
58. Sheskin DJ. Handbook of Parametric and Nonparametric Statistical Procedures (3rd ed). Chapman, Hall / CRC; 2004.
59. Simon SR, Evans JS, Benjamin A, Delano D, Bates DW. Patients' Attitudes toward Electronic Health Information Exchange: Qualitative Study. Journal of Medical Internet Research 2009; 11(3): e30.
60. Singer E, Hippler HJ, Schwarz N. Confidentiality Assurances in Surveys: Reassurance or Threat? Journal of Public Opinion Research 1992; 4(3): 256–268.
61. Singer E, von Thurn DR, Miller ER. Confidentiality Assurances and Re-sponse: A Quantative Review of the Experimental Literature. Public Opinion Quartaly 1995; 59 (1): 66–77.
62. Streiner DL, Norman GR. Correction for Multiple Testing: Is There a Resolution? Chest 2011; 140(1): 16–18.
63. Sultan N. Making Use of Cloud Computing for Healthcare Provision: Opportunities and Challenges. International Journal of Information Management 2014; 34(2): 177–184.
64. Sultan N. Discovering the Potential of Cloud Computing in Accelerating the Search for Curing Serious Illnesses. International Journal of Information Management 2014; 34(2): 221–225.
65. Teixeira PA, Gordon P, Camhi E, Bakken S. HIV Patients' Willingness to Share Personal Health Information Electronically. Patient Education and Counseling 2011; 84(2): e9-e12.
66. Terry A, Chesworth B, Stolee P, Bourne R, Speechley M. Joint Replacement Recipients' Post-Surgery Views about Health Information Privacy and Registry Participation. Health Policy 2007; 85: 293–304.
67. Thrall JS, McCloskey L, Ettner SL, Rothman ED, Tighe JE, Emans SJ. Confidentiality and Adolescents' Use of Providers for Health Information and for Pelvic Examinations. Archives of Pediatrics and Adolescent Medicine 2000; 154(9): 885–92.
68. Wallis LA, Fleming J, Hasselberg M, Laflamme L, Lundin J. A Smartphone App and Cloud-Based Consultation System for Burn Injury Emergency Care. PLoS One 2016; 11(2): e0147253.
69. Weng SJ, Lai LS, Gotcher D, Wu HH, Xu YY, Yang CW. Cloud Image Data Center for Healthcare Network in Taiwan. Journal of Medical Systems 2016; 40(4): 89.
70. Whetstone M, Goldsmith R. Factors Influencing Intention to Use Personal Health Records. International Journal of Pharmaceutical and Healthcare Marketing 2009; 3(1): 8–25.
71. Whiddett R, Hunter I, Engelbrecht J, Handy J. Patients' Attitudes towards Sharing Their Health Information. International Journal of Medical Informatics 2006; 75(7): 530–541.
72. Wilkowska W, Ziefle M. Privacy and Data Security in e-Health: Requirements from the User's Perspective. Health Informatics Journal 2012; 18: 191.
73. Zulman DM, Nazi KM, Turvey CL, Wagner TH, Woods SS, An LC. Patient Interest in Sharing Personal Health Record Information. Annals of Internal Medicine 2011; 155(12): 805–811.