UNDERSTANDING PHYSICIANS' ADOPTION OF HEALTH CLOUDS

Tatiana Ermakova

Department of Information and Communication Management,
Technical University of Berlin, Berlin
tatiana.ermakova@tu-berlin.de

ABSTRACT

Recently proposed health applications are able to enforce essential advancements in the healthcare sector. The design of these innovative solutions is often enabled through the cloud computing model. With regards to this technology, high concerns about information security and privacy are common in practice. These concerns with respect to sensitive medical information could be a hurdle to successful adoption and consumption of cloud-based health services, despite high expectations and interest in these services. This research attempts to understand behavioural intentions of healthcare professionals to adopt health clouds in their clinical practice. Based on different established theories on IT adoption and further related theoretical insights, we develop a research model and a corresponding instrument to test the proposed research model using the partial least squares (PLS) approach. We suppose that healthcare professionals' adoption intentions with regards to health clouds will be formed by their outweighing two conflicting beliefs which are performance expectancy and medical information security and privacy concerns associated with the usage of health clouds. We further suppose that security and privacy concerns can be explained through perceived risks.

KEYWORDS

Cloud Computing, Healthcare, Adoption, Physician, Security and Privacy Concerns

1. INTRODUCTION

Nowadays, healthcare and medical service delivery are on the way to be revolutionized ([7][7],[21]). Due to the recently proposed solutions, medical data can be easily shared and collaboratively used by healthcare professionals involved in the medical treatment [42][42], while novice surgeons can automatically be assisted in their surgical procedures [32][32] and physicians can be supported to make their therapy-related decisions [30][30]. The design of these apparently important innovative healthcare solutions is often enabled through the cloud computing model, which is known for providing adequate computing and storage resources on demand [33][33]. However, the immediate involvement of the cloud computing's third-party as well as communication via the open Internet landscape might lead to unexpected risks (e.g., legal problems) ([6][6],[35]) and therefore cause intense concerns among medical workers with respect to cloud computing companies' ability and willingness to protect disclosed medical information ([24], [36], [43]). While online medical service providers currently show interest in collecting medical information of their customers ([22][22],[25]), through the misuse of medical information the service users might get subject to harassment by marketers of medical products and services, and discrimination by employers, healthcare insurance agencies, and associates

David C. Wyld et al. (Eds) : ITCS, CST, JSE, SIP, ARIA, DMS - 2015
pp. 17–24, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.50102

([3][3],[27]). The exposure of security and privacy concerns related to sensitive medical information could be a serious hurdle to successful adoption and consumption of cloud-based health services, as repeatedly demonstrated by prior empirical evidence in other healthcare settings ([1][1], [2], [3], [18], [15], [29], [6], [35], and [5]).

This research examines which determinants can explain the extent to which medical workers will be willing to adopt health clouds in their daily work. To conduct the research, we follow the guidelines proposed by [44][44], [38], [31] and [19]. We build on well-established theories and works on adoption of information technologies ([47], [48]) and existing theoretical insights into the factors influencing healthcare IT and cloud computing adoption. We further draw on utility maximization theory ([3], [12]) arguing that one tries to maximize his or her total utility. We suppose the utility function to be given by the trade-off between expected positive and negative outcomes in a healthcare professional's decision-making process with regards to the usage of health clouds.

The paper is divided into four sections. In Section 2, we introduce the background of our research, highlight main theoretical foundations and formulate research hypothesis. Section 3 proceeds with presenting the research model where we illustrate the hypothesized relations. It further deals with the instrument developed to test the proposed research model using the partial least squares (PLS) approach ([19][19], [20], [44]). We conclude by recapitulating the results of this work, extensively discussing its limitations and thus giving recommendations for further research.

2. BACKGROUND AND THEORETICAL FOUNDATIONS

The availability of medical data is of utmost importance to physicians during the medical service delivery [42][42]. The healthcare sector can further profit from modern data analysis techniques. Their application fields in the healthcare area range from disease detection, disease outbreak prediction, and choice of a therapy to useful information extraction from doctors' free-note clinical notes, and medical data gathering and organizing [21]. These techniques can also be applied to assessment of plausibility and performance of medical services and medical therapies development [7]. Recently, [32] introduced an interactive three-dimensional e-learning portal for novice surgeons. Under real time conditions, their surgical procedures are to be compared to the practice of experienced surgeons. [30] presented a decision support system aimed to assist physicians in finding a successful treatment for some certain illness based on the currently available best practices and the characteristics of a given patient.

By provisioning adequate capacities to store and process huge amounts of data, cloud computing facilitates the design of these innovative applications in the healthcare area. However, this technology is also known for users' concerns about their information security and privacy ([24], [36]). While the providers of healthcare-related websites are interested in collecting medical information ([22][22], [25]), the misuse of medical information might result in different harassment and discrimination scenarios for patients ([3],[27]). In the recent past, there were cases where, based on disclosed medical information, marketers of medical products and services sent their promotional offers; employers refused to hire applicants and even fired employees; insurance firms denied life insurances. The exposure of the concerns surrounding information security and privacy could therefore negatively affect adoption and consumption of cloud-based health services, as multiple empirical studies demonstrated this in the healthcare context ([1], [2], [3][3], [18], [15], [29], [6], [35] and [5]) and other settings ([13], [14] and [40]).

In the present work, we try to understand the predictors of behavioural intention of healthcare professionals to adopt health clouds in their work. In the research related to management of

information systems (MIS), a variety of theories have been applied to explain an individual's adoption of information technologies. Among others, these include theories of reasoned action (TRA), planned behaviour (TPB), technology acceptance model (TAM), and unified theory of acceptance and use of technology (UTAUT) ([47], [48]). In line with these theories, we suppose that healthcare professionals' adoption of health clouds is a product of beliefs surrounding the system. We additionally assume that medical workers' intentions are consistent with utility maximization theory ([3], [12]) which posits that an individual attempts to maximize his or her total utility. As usage of health clouds is associated with numerous risks for a healthcare professional, we suppose that his or her utility function in the presented context is given by the calculus of conflicting beliefs which involve performance expectancy of the services, on one side, and associated security and privacy concerns about medical information, on the other side. We further postulate that information security and privacy concerns result from perceived risks.

2.1 Performance Expectancy

In one of the recent works on information technology acceptance, Venkatesh et al. [47] defines performance expectancy as the extent to which individuals believe that using the information technology is helpful in attaining certain gains in their job performance. Performance expectancy and other factors that pertain to performance expectancy such as perceived usefulness are generally shown to be the strongest predictors of behavioural intention [47]. Previous work suggests that healthcare professionals tend to be higher willing to adopt technological advances in their practice the higher they perceive their usefulness ([17], [8], [46], [35]). Similarly, cloud computing is more likely to be adopted the more beneficial it appears to the decision maker ([23], [28], [29], [36]). Therefore, we hypothesize that:

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

2.2 Security and Privacy Concerns

Online companies rely on use of their customers' personal information to select their marketing strategies ([36], [25]). As a result of this, Internet users view their privacy as being invaded. A recent survey revealed that 90% of Americans and Britons felt concerned about their online privacy and over 70% of Americans and 60% of Britons were even higher concerned than in the previous year [43].

Healthcare professionals appear to be ones of the most anxious Internet users in terms of information privacy. Dinev and Hart [13] argue that Internet "*users with high social awareness and low Internet literacy tend to be the ones with the highest privacy concerns*". Although this group of users constitute the intellectual core of society, they are not able or willing to keep up with protecting technologies while using the Internet. Simon et al. [39] further state that physicians are worried about patient privacy even more than the patients themselves.

In this study, privacy concerns are related to healthcare professionals' beliefs regarding cloud computing companies' ability and willingness to protect medical information ([40], [4], [36]). The dimensions of privacy concerns involve errors, improper access, collection, and unauthorized secondary usage.

Due to the open Internet infrastructure vulnerable to multiple security threats [36], we further consider security concerns. They refer to healthcare professionals' beliefs regarding cloud computing companies' ability and willingness to safeguard medical information from security breaches ([4], [36]). The dimensions of security concerns include information confidentiality and

integrity, authentication (verification) of the parties involved and non-repudiation of transactions completed.

Similarly to [4], we distinguish six dimensions of the combined security and privacy concerns, where we consider the dimensions of errors and improper access to be equivalent to the expectancy are to be measured with items adapted from Venkatesh et al. ([47], [48]). Security and privacy concerns are to be explored at a more detailed level, as recommended by [1]. With regards to the concerns, we draw on the multi-dimensional view proposed by Bansal [4]. The dimensions of privacy-related concerns, i.e., collection, errors, unauthorized secondary use, and improper access, originate from the work by Smith et al. [40] and were validated in healthcare privacy studies ([15], [18]). To measure the factors associated with collection, integrity/errors, and confidentiality/improper access, the questions from [18] were adapted. For the secondary use construct, we took items from [12]. Measures for the remaining underlying factors, i.e., authentication and non-repudiation, were developed based on [4]. To measure perceived risks, we rely on the items by [16].

Table 1. Research Model Constructs and Related Questionnaire Items

Construct	**Items**
Behavioural Intention to Adopt Health Clouds (based on [47], [48])	Given I get the system offered in the future and the patient consent for medical information transmission over the system is given, … … I intend to use it whenever possible. … I plan to use it to the extent possible. … I expect that I have to use it.
Performance Expectancy (based on [47], [48])	Using the system would make it easier to do my job. I would find the system useful in my job. If I use the system, I will spend less time on routine job tasks.
Security and Privacy Concerns – Integrity / Errors (based on [4], [40], [18])	I would be concerned that in the system… … medical information can be modified (altered, corrupted). … medical information is not enough protected against modifications. … accurate medical information can hardly be guaranteed.
Security and Privacy Concerns – Confidentiality / Improper Access (based on [4], [40], [18])	I would be concerned that in the system… … medical information can be accessed by unauthorized people. … medical information is not enough protected against unauthorized access. … authorized access to medical information can hardly be guaranteed.
Security and Privacy Concerns – Authentication (based on [4])	I would be concerned that in the system… … transactions with a wrong user can take place in the system. … verifying the truth of a user in the system is not enough ensured. … transacting with the right user in the system can hardly be guaranteed.
Security and Privacy Concerns – Nonrepudiation (based on [4])	I would be concerned that transactions in the system … …. could be declared untrue. … are disputable. … are deniable.
Security and Privacy Concerns – Collection (based on [4], [40], [18])	I would be concerned that medical information transmitted over the system … … does not get deleted from the cloud. … is kept as a copy. … is collected by the cloud provider.
Security and Privacy Concerns – Unauthorized Secondary Use (based on [4], [40], [12])	I would be concerned that medical information transmitted over the system can be … … used in a way I did not foresee. … misused by someone unintended. … made available/sold to companies or unknown parties without your knowledge.

Perceived Risks (based on [16])	In general, it would be risky to transmit medical information over the system. Transmitting medical information over the system would involve many unexpected problems. I would not have a good feeling when transmitting medical information over the system.

The respondents are supposed to be presented one of the above mentioned scenarios. They further will be asked to provide their answers to the questions on a 7 Likert scale (e.g., 1: Not likely at all, 2: Highly unlikely, 3: Rather unlikely, 4: Neither likely nor unlikely, 5: Rather likely, 6: Highly likely, 7: Fully likely). Additionally, they will be asked about practice period [9], their workplace location (e.g. rural or urban) ([35], [9]), gender, and age, etc. [35]. These questions will mainly allow describing the sample.

3. CONCLUSION, LIMITATIONS AND SUGGESTIONS FOR FUTURE RESEARCH

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

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

Our work implies some limitations. First, there might be some other possible casual relationships between the constructs proposed in the research model. For example, [46] hypothesize that EMR security/confidentiality influences its perceived usefulness, while [17] find a positive relationship between perceived importance of data security and perceived usefulness of electronic health services. As identified by [26], perceived privacy risk directly influences personal information disclosure in the context of online social networks. In our future research, we are going to verify all possible paths, as recommended by [20].

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

Venkatesh et al. [47] define effort expectancy as referring to the extent to which an individual finds the system easy to use. The factor is also captured by perceived ease of use specified in TAM. Perceived ease of use is important for potential cloud computing users ([28], [36]). Physicians view easy-to-use services as more useful and stronger intend to use them ([17], [6], [35], [6]). Contrary to these findings and other previous research assertions (e.g., [47], [48]), perceived ease of use did not exert any significant effects on perceived usefulness or attitude, when tested in the telemedicine context [8]. The authors suggest that physicians comprehend new information technologies more easily and quickly than other user groups do. Alternatively, the importance of perceived ease of use may be weakened by increases in general competence or staff assistance [8]. These aspects are implied in the concept of facilitating conditions which relates to the extent to which individuals believe in the existence of an organizational and technical

infrastructure to support their system use [47]. They were found to play a role in formation of behavioural intention to use cloud computing in hospital [29] and perceived usefulness of healthcare information technologies ([8], [34], [6], [35]).

Social influence refers to the degree to which individuals perceive that others' beliefs about their system use are important [47]. Being differently labelled across studies, social influence was found to have contradictory results when tested with regards to behavioural intention. Cloud computing users were significantly guided by the way they believe they are viewed by others as having used the cloud computing technology [28]. However, practicing physicians' intentions to use telemedicine technology were not significantly influenced by social norms [8]. Dinev and Hu [11] observe subjective norm influencing behavioural intention rather for IT aware groups. Dinev and Hu believe that the more IT knowledgeable the group are, the more they communicate about IT related issues and are willing to learn IT solutions their peers already use.

Finally, some variables which are to be used to describe the sample (e.g., workplace location) can further be controlled for their role. As observed by [35], urban hospitals could be expected to adopt innovative solutions rather than rural ones. Hospitals located outside cities and towns are the only alternative for people living nearby. So they do not have to compete with others in adopting new technologies. Furthermore, they are typically under-occupied and have little financial support.

ACKNOWLEDGEMENTS

The work presented in this paper was performed in the context of the TRESOR research project [42]. TRESOR is funded by the German Federal Ministry of Economic Affairs and Energy (BMWi).

REFERENCES

[1] Angst, C.M. & Agarwal, R. (2009) "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion", *MIS Quarterly*, Vol. 33, No. 2, pp. 339-370.

[2] Bansal, G., Zahedi, F. & Gefen, D. (2007) "The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online", *Americas Conference on Information Systems*.

[3] Bansal, G., Zahedi, F. & Gefen, D. (2010) "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online", *Decision Support Systems*, Vol. 49, No. 2, pp. 138-150.

[4] Bansal, G. (2011) "Understanding the Security in Privacy-Security Concerns: A Theoretical and Empirical Examination", *Americas Conference on Information Systems*.

[5] Bassi, J., Lau, F. & Lesperance, M. (2012) "Perceived Impact of Electronic Medical Records in Physician Office Practices: A Review of Survey-Based Research", *Interactive Journal of Medical Research*, Vol. 1, No. 2, e3.

[6] Boonstra, A. & Broekhuis, M. (2010) "Barriers to the Acceptance of Electronic Medical Records by Physicians from Systematic Review to Taxonomy and Interventions", *BMC Health Services Research*, Vol. 10, No. 231.

[7] BMWi (2014) "Anwendungen für den Gesundheitssektor", http://www.trusted-cloud.de/239.php, accessed November 6, 2014.

[8] Chau, P.Y.K. & Hu, P.J.-H. (2001)"Information Technology Acceptance by Individual Professionals: A Model Comparison Approach", *Decision Sciences*, Vol. 32, No. 4, pp. 699–719.

[9] DesRoches, C.M., Campbell, E.G., Rao, S.R., Donelan, K., Ferris, T.G., Jha, A., Kaushal, R, Levy, D.E., Rosenbaum, S., Shields, A.E. & Blumenthal, D. (2008) "Electronic Health Records in Ambulatory Care – A National Survey of Physicians", *The New England Journal of Medicine*, Vol. 359, No. 1, pp. 50-60.

[10] Dinev, T. & Hart, P. (2004) "Internet Privacy Concerns and their Antecedents - Measurement Validity and a Regression Model", *Behaviour & Information Technology*, Vol. 23, No. 6, pp. 413-422.
[11] Dinev, T. & Hu, Q. (2005) "The Centrality of Awareness in the Formation of User Behavioral Intention Toward Preventive Technologies in the Context of Voluntary Use", *Conference for Special Interest Group on Human-Computer Interaction*.
[12] Dinev, T. & Hart, P. (2006) "An Extended Privacy Calculus Model for E-Commerce Transactions", *Information Systems Research*, Vol. 17, No. 1, pp. 61–80.
[13] Dinev, T. & Hart, P. (2006) "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact", *International Journal of E-Commerce*, Vol. 10, No. 2, pp. 7-29.
[14] Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. & Colautti, C. (2006) "Internet Users' Privacy Concerns and Beliefs about Government Surveillance: an Exploratory Study of Differences between Italy and the United States", *Journal of Global Information Management*, Vol. 14, No. 4, pp. 57–93.
[15] Dinev, T., Albano, V., Xu, H., D'Atri, A. & Hart, P. (2012) "Individual's Attitudes Towards Electronic Health Records – A Privacy Calculus Perspective", *Annals of Information Systems*.
[16] Dinev, T., Xu, H., Smith, H.J. & Hart, P. (2013) "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts", *European Journal of Information Systems*, Vol. 22, No. 3, pp. 295-316.
[17] Dünnebeil, S., Sunyaev, A., Blohm, I., Leimeister, J.M. & Krcmar, H. (2012) "Determinants of Physicians' Technology Acceptance for e-Health in Ambulatory Care", *International Journal of Medical Informatics*, Vol. 81, No. 11, pp. 746-760.
[18] Ermakova, T., Fabian, B., & Zarnekow, R. (2014) "Acceptance of Health Clouds – a Privacy Calculus Perspective", *European Conference on Information Systems*.
[19] Gefen, D., Straub, D.W. & Boudreua, M.C. (2000) "Structural Equation Modeling and Regression: Guidelines for Research Practice", *Communications of the Association for Information Systems*, Vol. 4, No. 7, pp. 1-78.
[20] Gefen, D., Rigdon, E. & Straub, D. (2011) "An Update and Extension to SEM Guidelines for Administrative and Social Science Research", *MIS Quarterly*, Vol. 35, No. 2, pp. iii-xiv.
[21] Hardesty, L. (2013) "Big Medical Data", http://web.mit.edu/newsoffice/2013/big-medical-data-0125.html, accessed November 8, 2014.
[22] Huesch, M. D. (2013) "Privacy Threats when Seeking Online Health Information", *JAMA Internal Medicine*, Vol. 173, No. 19, pp. 1838-1840.
[23] Hsu, P.-F., Ray, S. & Li-Hsieh, Y.-Y. (2014) "Examining Cloud Computing Adoption Intention, Pricing Mechanism, and Deployment Model", *International Journal of Information Management*, Vol. 34, No. 4, pp. 474–488.
[24] Ion, I., Sachdeva, N., Kumaraguru, P. & Capkun, S. (2011) "Home is Safer than the Cloud! Privacy Concerns for Consumer Cloud Storage", *Symposium on Usable Privacy and Security*.
[25] Kaletsch, A. & Sunyaev, A. (2011). "Privacy Engineering: Personal Health Records in Cloud Computing Environments". *International Conference on Information Systems*.
[26] Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrandt, T. (2009) "Online Social Networks: Why We Disclose", *Journal of Information Technology*, Vol. 25, No. 2, pp. 109–125.
[27] Laric, M.V., Pitta, D.A. & Katsanis, L.P. (2009) "Consumer Concerns for Healthcare Information Privacy: A Comparison of U.S. and Canadian Perspectives", *Research in Healthcare Financial Management*, Vol. 12, No. 1, pp. 93-111.
[28] Li, Y. & Chang, K.-C. (2012) "A Study on User Acceptance of Cloud Computing: A Multi-Theoretical Perspective", *Americas Conference on Information Systems*.
[29] Lian, J., Yen, D.C. & Wang, Y. (2014) "An Exploratory Study to Understand the Critical Factors Affecting the Decision to adopt Cloud Computing in Taiwan Hospital", *International Journal of Information Management*, Vol. 34, No. 1, pp. 28-36.
[30] Lupse, O. S., Stoicu-Tivadar, L. & Golie, C. (2013) "Assisted Prescription Based on Successful Treatments", *E-Health and Bioengineering Conference*.
[31] MacKenzie, S.B., Podsakoff, P.M. & Podsakoff, N.P. (2011) "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques", *MIS Quarterly*, Vol. 35, No. 2, pp. 293-334.
[32] Mani, G. & Li, W. (2013) "3D Web Based Surgical Training Through Comparative Analysis", *International Conference on 3D Web*.
[33] Mell, P. & Grance, T. (2012). "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed March 12, 2014.

[34] Moores, T.T. (2012) "Towards an Integrated Model of IT Acceptance in Healthcare", *Decision Support Systems*, Vol. 53, No. 3, pp. 507-516.
[35] Najaftorkaman, M. & Ghapanchi, A.H. (2014) „Antecedents to the User Adoption of Electronic Medical Record", *Pacific Asia Conference on Information Systems*.
[36] Opitz, N., Langkau, T.F., Schmidt, N.H. & Kolbe, L.M. (2012) "Technology Acceptance of Cloud Computing: Empirical Evidence from German IT Departments", *Hawaii International Conference on System Sciences*.
[37] Pavlou, P., Liang, H. & Xue, Y. (2007) "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principle–Agent Perspective?", *MIS Quarterly*, Vol. 31, No. 1, pp. 105–136.
[38] Petter, S., Straub, D. & Rai, A. (2007) "Specifying Formative Constructs in Information Systems Research", *MIS Quarterly*, Vol. 33, No. 4, pp. 623-656.
[39] Simon, S.R., Kalshal, R., Cleary, P.D., Jenter, C.A., Volk, L.A., Oray, E.J., Burdick E., Poon, E.G. & Batees, W.W. (2007) "Physicians and Electronic Health Records: A Statewide Survey", *Archives of Internal Medicine*, Vol. 167, No. 5, pp. 507-512.
[40] Smith, H.J., Milberg, J.S. & Burke, J.S. (1996) "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly*, Vol. 20, No. 2, pp. 167-196.
[41] European Parliament and Council (1995) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data", *Official Journal*, Vol. 281, No. 31, pp. 31 – 50.
[42] TRESOR (2014) "TRESOR", http://www.cloud-tresor.com/, accessed November 6, 2014.
[43] TRUSTe (2014) "TRUSTe", http://www.truste.com/, accessed August 19, 2014.
[44] Urbach, N. & Ahlemann, F. (2010) "Structural Equation Modeling in Information Systems Research Using Partial Least Squares", *Journal of Information Technology Theory and Application*, Vol. 11, No. 2, pp. 5-40.
[45] U.S. Department of Health & Human Services (1996) "Health Insurance Portability and Accountability Act of 1996 (HIPAA)", http://www.hhs.gov/ocr/privacy/, accessed December 3, 2014.
[46] Vathanophas, V. & Pacharapha, T. (2010) "Information Technology Acceptance in Healthcare Service: The Study of Electronic Medical Record (EMR) in Thailand", *Technology Management for Global Economic Growth*.
[47] Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003) "User Acceptance of Information Technology: Toward a Unified View", *MIS Quarterly*, Vol. 27, No. 3, pp. 425–478.
[48] Venkatesh, V., Thong, J.Y.L. & Xu, X. (2012) "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology", *MIS Quarterly*, Vol. 36 No. 1, pp. 157-178.
[49] Xu, H., Dinev, T., Smith, H. J. & Hart, P. (2008) "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View", *International Conference on Information Systems*.
[50] Xu, H., Dinev, T., Smith, H. J. & Hart, P. (2011) "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances", *Journal of the Association for Information Systems*, Vol. 12, No. 12, pp. 798-824.

AUTHOR

Tatiana Ermakova is a research assistant at the Department of Information and Communication Management of the Technical University of Berlin. She holds a bachelor degree in Economics and a diploma degree in Applied Informatics in Economics from the Russian Academy of Economics, a M.Sc. in Information Systems from Humboldt University of Berlin.