Patient Adoption of Accountable Care Organization Cloud Platforms Amidst Privacy and Paid Access Concerns:

Investigating the Role of Information Ownership and Paid Access

Pamella Howell
Management Science and Systems
University at Buffalo
Buffalo, United States
pamellah@buffalo.edu

Victoria Kisekka
Information Security and Digital Forensics
University at Albany
Albany, United States
vkisekka@albany.edu

Abstract—Current trends suggest that the use of cloud computing platforms in the healthcare industry is on the rise. However, adoption of cloud services amongst patients has been slow. It is due, in part, to privacy concerns and the uncertainties surrounding information ownership on the cloud. This research investigates patients’ willingness to adopt ACO cloud computing platforms amidst privacy concerns. We adopt the privacy calculus model, and contribute to theory by adding two new constructs: health information ownership and paid access to cloud services.

Keywords—privacy; electronic health records; cloud computing; information ownership; paid access; accountable care organizations

I. INTRODUCTION

Information ebbs and flows freely across the Internet through social media and other mediums, yet individuals care about preserving the privacy of their data. The same goes for health information; people expect privacy when they visit online healthcare communities for support or browse health websites for answers. In practice, healthcare practitioners must provide the same privacy assurances for electronic protected health information they generate in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its HIPAA Security Rule [1]. The Health Insurance Technology for Economic and Clinical Health (HITECH) Act [1]. The HITECH Act reinforced the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulation [2]. Since the enactment of HITECH, the government launched additional initiatives to protect and capitalize on the increased use of health Information Technology (IT) artifact [7]. Thus, the central focus of this study is to assess the impact of privacy concerns on patients’ intention to consent to a healthcare cloud-based services within an ACO.

We investigate patients’ adoption of accountable care organizations’ cloud computing platforms amidst privacy concerns. We adopt the privacy calculus model [8] which explains the specific conditions that influence individuals’ choice to accept a certain level of privacy in exchange for perceived benefits. Our theoretical contribution comes from the extension of the privacy calculus model to include variables unique to the adoption of a cloud-based health record platform, namely, information ownership, and paid access to cloud platforms. Additionally, we refine the privacy concern and trust constructs by taking into consideration two levels of information control that are relevant to cloud computing [9]; information control by the ACO network, and information control by the cloud service providers. This research in progress has several practical contributions for guiding ACO networks in the development of patient-centered privacy policies when implementing cloud-based platforms. The research also has implications for improving patients’ adoption of ACO cloud computing platforms.

II. THEORETICAL FRAMEWORK AND LITERATURE REVIEW

The demand for cloud computing resources has increased since the inception of pay-as-you-go cloud computing services in the mid-2000s. Specific applications of cloud computing
within healthcare include e-prescription, electronic health record, telemedicine, medical imaging, remote connections with physicians, self-management, and body sensor networks [10]. Cloud-based e-health is also used to manage access to personal health records such as Microsoft HealthVault [11]. Researchers have explored cloud-based health services beyond its general applicable uses. As an example, authors like Bernsmed et al. (2013) evaluate the factors affecting adoption of cloud-based health records in the public health domain. Due to limited knowledge, additional studies are required to assess adoption in private healthcare organizations. This research addresses that limitation.

An assessment of extant literature shows that the privacy paradox explored by Dinev and Hart [8] and numerous scholars persists in healthcare. The privacy paradox affects the adoption and use of cloud computing in healthcare and is explained by the calculus theory whereby a participant will forgo some degree of privacy if they receive a particular benefit [13, 14]. Despite the value of cloud-based health platforms, people exhibit privacy concerns when transferring data via the Internet [8, 15, 16].

Privacy scholars propose that before disclosing information people determine whether it will be used fairly, and seek assurances that they will not suffer negative consequences [16, 17]. Any perceived adverse effects will negatively affect the individual’s intention to use cloud-based services. In the same way, patients will assess the privacy risks associated with ACO cloud-based platform prior to adopting them. Scholars have traditionally focused on technical solutions such as data encryption and network security mechanisms [18], with limited attention paid to patients’ preferences.

The dependent variable we study is a patient’s intention to adopt ACO cloud-based platforms. We adopt the privacy calculus model [8] which explains the specific conditions that influence individuals’ choice to accept a certain level of privacy in exchange for perceived benefits. We investigate the influence of information ownership, paid access to cloud services, privacy concerns, trust, and personal cloud interest, on intention to adopt ACO cloud-based platforms. This research makes a theoretical contribution by adding two new constructs to the original privacy calculus model. The next paragraphs discuss each construct in detail.

A. Information Ownership

Information ownership pertains to having the legal right to control a specified piece of data. An information owner has the right to create, edit, secure, and limit access the information. According to HIPAA regulation, the information collected on patients is owned by the insurance company or healthcare provider. Patients do not own their health records; but, they are permitted under HIPAA to have unlimited access to their files upon request. Like many other government policies, patients are often unaware of the ownership rule regarding their health information records [15, 18, 19]. Rodrigues et al. (2013) and Karran et al. (2015) underscore this concern by showing that there is a prevalence of uncertainty on information ownership. Scholars, therefore, recognize there are some gray areas regarding consumer cloud information ownership in the absence of a business contract [19].

This research addresses the gap by evaluating a person’s perception of information ownership and its impact on the intention to adopt a cloud computing. In instances where data ownership is clearly established, users are willing to adopt and utilize cloud computing services. For example, mobile device users who own digital information on iCloud and iTunes make up 27% of the cloud storage market share [20]. Suggesting that when people own information, as is the case with iCloud, iTunes, Dropbox, and similar cloud platforms, they utilize cloud services to store and manage their information. We argue that patients will behave similarly when they have a high perception of information ownership. In other words, the perception of health information ownership will drive the need for a patient to use cloud computing ACO platforms to manage their health data. The perceived benefit of controlling personal health information would negate privacy concerns associated with cloud computing ACO platforms.

Hypothesis 1. Perceived information ownership will be positively associated with behavioral intention to adopt ACO cloud-based platforms (Fig. 1.)

B. Paid Access

According to Tang et al. (2006), patients should pay to have access to medical records because paying for a service positively influences the perceived value of that service [22]. Price optimization studies for data storage suggest otherwise [23, 24]; Specifically, users are price sensitive when it comes to paying for tiered-storage services. A high price for data storage forces users to opt for cheaper storage options even when such options may provide less effective security compared to the top-tier, higher priced storage options [24]. In the same way, patients’ willingness to pay for cloud-based health services may be hindered by high prices. If cloud-based services with the most effective security controls are highly priced, patients may opt for cheaper options; thus, surrendering a certain level of privacy due to financial constraints. The introduction of an access fee may reduce the user’s willingness to participate on a cloud platform for cost sensitive patients. On the contrary, if paying for the medical records increases the sense of ownership in the ACO cloud computing platform then individuals might be more willing to participate. The increased sense of ownership comes from the investment made for accessing the system. To evaluate the impact of paid access we developed two hypotheses:

Hypothesis 2a. Paid access for ACO cloud platforms is negatively associated behavioral intention to adopt ACO cloud-based platforms.

C. Perceived Cloud Computing Privacy Risk (PCR)

Privacy risk is the “potential loss of control over personal information” [25]. We defined PCR as a user’s belief in the likelihood of privacy loss associated with the use of cloud computing services. It is common for providers to share patient’s personal information to facilitate the provision of medical care. Despite the recognized benefits of information sharing, however, many users believe that sharing of personal
information increases privacy risks [26]. This is due in part to the increasing sophistication and advancement of data breaches. A data breach would result in negative consequences such as identity theft, unsolicited mail, and other unauthorized opportunistic uses of personal information. Related work in this area has shown that users’ perceived privacy risk is negatively related to the intention to disclose information [8]. Consistent with these findings, we argue that in the context of cloud computing, perceptions of privacy risk increase the likelihood that a patient will engage in preventative behavior to mitigate the risk. Here, we focus on the privacy risk associated with cloud computing in general.

Hypothesis 3: Perceived cloud computing privacy risk will be negatively associated with the behavioral intention to adopt ACO cloud platforms.

D. Cloud Computing Privacy Concerns

Privacy concern is a critical construct in the privacy calculus model. In the calculus model, privacy risk positively impacts internet privacy concerns [8]. We argue that perceived cloud computing privacy risk will have a similar effect on perceived cloud computing privacy concerns. The term privacy concerns is used herein to refer to the effectiveness of privacy preserving controls as perceived by the user. Patients’ privacy concerns inhibit the adoption of healthcare technologies and their willingness to share personal information [27]. These concerns stem from the fear of privacy loss due to ineffective privacy controls. Furthermore, there is a likelihood of information being lost, stolen, or leaked due to violations of security and privacy policies by employees. Thus, the level of uncertainty regarding the effectiveness of privacy preserving controls is increased by increasing cloud computing privacy risks.

In cloud computing, there is no ‘one size fits all’ security solution because cloud data is managed at two different levels of control [9]. The first level deals with the patient data managed by the ACO. The second level of control is by the cloud service provider. As discussed in Coles-Kemp, Reddington and Williams [9], cloud service vendors provide subscription services directly to patients, affording them anytime access to their personal medical data, and also the ability to control access to it. This research focuses on two aspects of privacy concerns: perceived cloud computing privacy concerns regarding the ACO cloud platform and privacy concerns regarding the cloud service provider.

Hypothesis 4a: Perceived cloud computing privacy risk will be positively associated perceived cloud computing privacy concerns regarding the ACO cloud platforms.

Hypothesis 4b: Perceived cloud computing privacy risk will be positively associated perceived cloud computing privacy concerns regarding the cloud service provider.

As stated previously, patients are not willing to share their information due to concerns regarding the secure handling of sensitive information by organizations [27]. Thus:

Hypothesis 5a: Perceived cloud computing privacy concerns regarding the ACO cloud platform will be negatively associated with the behavioral intention to adopt ACO cloud platforms.

Hypothesis 5b: Perceived cloud computing privacy concerns regarding the cloud service provider will be negatively associated with the behavioral intention to adopt ACO cloud platforms.

E. Trust

All robust privacy calculus models include a trust construct [8, 28]. Trust pertains to one’s expectation that his/her information will be handled safely, reliably, and competently. An individual who is confident that his/her information will not be used in opportunistic behavior is more likely to willingly disclose personal information compared to an individual who does not [8, 28]. We suggest that trust and intention to adopt ACO cloud platform are positively linked. Similar to privacy concerns, we focus on two aspects of trust: trust in ACO, and trust in cloud service provider.

Hypothesis 6a: Trust in the ACO cloud platforms will be positively associated with the behavioral intention to adopt ACO cloud platforms.

Hypothesis 6b: Trust in the cloud service provider will be positively associated with the behavioral intention to adopt ACO cloud platforms.

The antecedent of trust beliefs is risk [8, 29]. Lower levels of risk increase trust. This means when the perceived likelihood of cloud computing privacy loss is low, users will likely feel confident; trusting that the cloud computing service providers will be less likely to use information in an opportunistic behavior.

Hypothesis 7a: Perceived cloud computing privacy risk will be negatively associated with trust in the ACO cloud platforms.

Hypothesis 7b: Perceived cloud computing privacy risk will be negatively associated with trust in the cloud service provider.

F. Personal Cloud Computing Interest (PCI)

When people have a general interest in using a product or service, the likelihood of adopting similar products or services is high, regardless of the associated risks. Patients with a personal interest in cloud computing technologies are, therefore, more likely to adopt cloud services provided by their ACO notwithstanding the privacy concerns. This leads us to hypothesize that increased general interest in cloud services will override privacy concerns, resulting in increased cloud computing ACO platform adoption.

Hypothesis 8. Personal cloud computing interest will be positively associated with the behavioral intention to adopt ACO cloud platforms.
III. METHODOLOGY AND CONCLUSION

Initial data collection will take place using M-Turk to assess the viability of measures being developed for evaluation of patient privacy and security concerns for the adoption and use of cloud-based electronic health records. Measures will be developed following the principles of MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011) and Hinkin, T.R. 1998. The refined measure will be administered to patients currently enrolled in Accountable Care Organizations in the Eastern Region of the United States. The collected data will be analyzed using structural equation modeling techniques (AMOS and STATA) after testing for the standard assumptions of regression. This research in progress underscores the importance of information ownership and paid access on privacy concerns when an ACO networks develops patient-centered cloud-based platforms.

ACKNOWLEDGMENT

We would like to thank the reviewers for their insightful comments.

REFERENCES


