Decision Support Systems 57 (2014) 376–386

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract

Han Li [a], Ashish Gupta [b,*], Jie Zhang [c], Rathindra Sarathy [d]

[a] Minnesota State University Moorhead, USA
[b] University of Tennessee Chattanooga, USA
[c] Midwestern State University, USA
[d] Oklahoma State University, USA

ARTICLE INFO

Available online 6 November 2012

Keywords:
Personal health records
PHR
Privacy calculus
Perceived privacy control
Trust

ABSTRACT

Despite the growing research interest in the digitization of healthcare, current understanding of barriers to using health IT is mostly centered on providers. There is a lack of understanding of how to get patients involved in managing their own digital health information using standalone Personal Health Record Systems (PHR). To fill this research gap, this study proposes a trust-enabled fair social contract model to theorize and empirically test how individuals' intention to use standalone PHR is driven by a trust-enabled privacy calculus, buttressed by the level of perceived privacy control over their own health information and trust. The perceived benefits of using a standalone PHR, perceived privacy control and trust were found to be the major factors determining intention to adopt the PHR, overriding the effect of potential privacy risks of PHR. In addition, the results of the study suggest that the effect of perceived privacy control varies based on one's prior experience of falling victim to privacy invasions.

1. Introduction

Traditional paper-based documentation of medical records is error-prone and inefficient. Medical errors cause between 44,000 and 98,000 deaths each year, of which over 50% are avoidable [31]. Also, patients often receive unnecessary duplicate tests since paper-based patient data are not easily transferred among different healthcare providers. Health IT has been advocated as a means for improving efficiency, quality and safety of healthcare, and eventually curbing the hiking healthcare cost [28]. Health IT could potentially prevent thousands of errors, and save about $80 billion each year in the United States if it is widely adopted [29]. The healthcare industry is under the pressure to go through a digital transformation. The recent economic recovery package of the Obama administration will pay physicians $44,000 to $64,000 for adopting and effectively using EHRs from 2011 to 2015 [52]. Considerable research has been devoted to examining the impact of electronic health record systems (EHRs) and how to motivate healthcare providers such as physicians and hospitals to use EHRs [10,57]. However, the role of healthcare *consumers* in the wide deployment of health IT is largely overlooked. Besides hospitals and physicians, the participation of healthcare consumers in the digital transformation of healthcare industry is critical to its acceptance and success. Although, under HITEC and HIPAA acts, patients have indirect access to their medical records that are stored in various clinical databases such EMR systems through their care provider, the availability and convenient access to a complete portfolio of patient records for their own use remain limited. Such information exists in different formats (images, pdf, report, etc.) and is held in various clinic-owned databases such as (proprietary or customized) EMR systems, pharmaceutical health information systems (PHIS), radiology information systems (RIS), etc. In addition, personal health information may also be scattered in various hospitals, if the patient received care at multiple clinics. Generally, these clinics and hospital-owned databases don't have mechanism in place that allows for easy exchange of information among them, making it even more difficult for patients to access, manage and track their own health. This lack of an easy access to personal health records poses an even bigger challenge for patients suffering from chronic ailments that last over long time periods. Chronic diseases account for 75% of the nation's health care dollars [6]. The care of chronic diseases requires ongoing monitoring of patients' condition and communication between patients and their healthcare providers, making convenient and continuous access to medical records a critical need. All these highlight the importance of adopting PHR systems where patients take ownership of managing their personal records. This also reflects a paradigm shift in how patient information is being maintained, i.e. patient information not simply existing in care provider managed databases but also in patient managed datasets such as PHR systems [35].

Two types of personal health records systems (PHR) have been implemented to provide patients access to their personal health records and enable them to actively manage their own health information [52]. One is the *integrated* PHR, which is an extension of

* Corresponding author.
E-mail address: gupta@utc.edu (A. Gupta).

0167-9236/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2012.10.043

physicians' EHRs or a portal to data stored in EHRs. Another type is the *standalone* PHR systems such as Microsoft HealthVault, that are developed by online commercial companies. A standalone PHR is web-based, empowering patients with control of their own personal health data. Patients can gather, store and manage their health records using a standalone PHR and easily share the data with any healthcare provider. Online PHR is particularly valuable in case of emergencies when the hospital can be informed about a patient's current and past medication history expeditiously.

PHR is an emerging health IT. In a recent literature survey paper, Goldzweig et al. [28] emphasized the need for research into patient-focused IT applications. Currently, there is little theory-based scholarly research on PHR. Ozdemir et al. [44] examined the switching cost of patients' using PHR. Whetstone and Goldsmith [56] applied the TAM model [17] to investigate factors that influence intention to use PHR. However, the acceptance of PHR by patients is still a largely untapped research area. To fill the research gap, this study focuses on standalone PHR as it requires more active involvement from patients than an integrated PHR. We extend a privacy calculus model to examine factors that influence patients' willingness to use standalone PHR.

Consumers face serious threats to the privacy of their health information when such information is captured and stored digitally. In 2009, five computers and a flash drive containing medical records of about 10,000 individuals were stolen in Detroit [25]. A standalone PHR as a Web-based service may be hacked, exposing patients' health information to unauthorized access. To use PHR, one of the major barriers consumers have to overcome is their concern over information privacy. Patients may refuse to have their health records digitized due to privacy concerns [2]. A national survey conducted by the California Healthcare Foundation found that 67% of people are concerned about the privacy of their personal medical records [5]. Therefore, information privacy should play a key role in consumers' decision to use standalone PHR.

Consumers' privacy-related decisions have been widely considered to arise from a cost–benefit analyses or a "privacy calculus" [16,19]. In this study, we adopted a social contract perspective to understand the privacy calculus influencing individuals' decision to use standalone PHR. The privacy calculus is posited to be embedded in a trust-enabled social contract between the PHR vendor and the consumer reflecting the level of perceived control the consumer has over the privacy of their health data. In particular, our research questions are: 1) what are the benefits in the privacy calculus that factor into individuals' decision to use standalone PHR? 2) how does perceived privacy control act as a fairness lever adjusting the cost–benefit tradeoff analysis? and 3) how do preexisting trust beliefs in online vendors influence individuals' adoption decision?

2. Theoretical foundation

Prior studies have suggested that the effect of information privacy is malleable with situational stimuli [2,37]. Unable to achieve absolute information privacy, consumers often make a situational tradeoff when deciding whether to disclose their information to receive certain benefits. For example, online shoppers would have to disclose some personal information to complete ecommerce transactions. Similarly for standalone PHR, people would need to agree to build their medical profiles online and share them with healthcare providers to receive necessary medical care. It is important to examine individuals' intention to use standalone PHR in an exchange context as a privacy calculus involving assessments of competing exchange benefits and privacy risks. Individuals need to weigh the benefits of PHR against risks of storing and managing their health information over the Internet. They would be more likely to use standalone PHR if the privacy risks could be overridden by the benefits of PHR. We further integrate this calculus perspective with that of a social contract to better understand the privacy cost–benefit tradeoffs involving highly sensitive personal health data and the adoption of embryonic health IT. The perspective of a social contract allows us to have a fine-grained examination of the privacy calculus specific to the exchange of highly sensitive personal health information and incorporate the role of trust and fairness into the privacy calculus framework. Thus, we propose that the privacy calculus associated with health data disclosure is embedded in a social contract with trust as the central bond and privacy control as a lever signaling the procedural fairness of health information exchange.

2.1. Information privacy and calculus perspective

Information privacy refers to the ability of individuals to control when, how, and to what extent their personal information is exchanged with and used by others [16,50,55]. The issue of information privacy arises when information is exchanged to enable the primary transaction involving acquisition of products or services. During the information exchange, consumers' decision of whether to share private information or not involves a privacy calculus, where privacy risks are weighed against exchange benefits [16]. The concept of a privacy calculus has received consistent empirical support in prior research [19,37,60]. However, specific forms of privacy calculus and their effect on privacy decisions may vary depending on the context of technologies. In this study, we further tailor the privacy calculus to the context of adoption standalone PHR. In particular, we identified and empirically tested several benefits of PHR technology to find specific benefits that factor into individuals' decision to use standalone PHR. In addition, people are particularly sensitive about the privacy of their health records [2]. Personal health records in digital form may aggravate people's privacy concern over the potential misuse of their health records. Thus, the decisions to adopt standalone PHR would involve a highly salient privacy calculus in which consumers actively assess the competing privacy risks and benefits.

2.2. Information exchange and social contract

Besides the calculative assessment of competing risks and benefits, personal information exchange is also affected by the fairness of the social contract, when the exchange involves unknown consequences [16,36,37,41]. The underlying assumption of a social contract is bounded moral rationality, i.e. "individual moral agents lack the information, time, and emotional strength to make perfect judgments" [20, p. 18]. The disclosure of personal health information to companies providing standalone PHR is highly susceptible to such bounded moral rationality. Individuals often do not have complete information for judging the benefits and risks of using PHR. For example, the vendor may disclose the health information to a third party without the awareness of patients or use patients' information to conduct marketing activities not authorized by patients. Thus, the uncertain nature of personal health information exchange is consistent with the assumptions of the social contract, demanding the existence of an *implicit* social contract to govern information exchange.

A social contract consists of shared norms or understanding about the rights and responsibilities between two parties in an exchange relationship [21]. The underlying norms in a social contract are context-specific, i.e. varying with the situation of the exchange. For information exchange, some basic norms identified in prior studies are organizations' social obligations to respect consumer information privacy, [30] and the understanding of risks and returns in the exchange by the two parties entering into the social contract [9]. Therefore, the social contract governing information exchange involves a privacy-related cost–benefit analysis or has the privacy calculus built into it. Alternatively, we can view the privacy calculus as being embedded in a social contract.

The rights and responsibilities in a social contract are neither defined explicitly in advance nor enforced through laws. Instead, a social contract is implicit, which is formulated and executed in the