The Role of Security Beliefs in the Use of Personal Health Records (PHR)

Emergent Research Forum (ERF)

Mohamed Abdelhamid
California State University Long Beach
Mohamed.abdelhamid@csulb.edu

Spyridon Samonas
California State University Long Beach
Spyro.Samonas@csulb.edu

Abstract

The patient-centered approach to healthcare requires integrating patient values, beliefs, and culture, in the clinical decision-making process. Personal Health Records (PHR) are recognized by patients as a way to improve the experience of health care for themselves and their families. PHR contain information about a patient’s health, and it is compiled and maintained by the patient. In addition, PHR can exchange information with a health information exchange. This allows patients persistent access to complete health information. With the use of PHR, patients may share their health records with people they choose. Revoking access at any time is also under the patients’ control. PHR systems are relatively new, and hence, their diffusion is currently growing rapidly in the U.S. For this reason, while there is a significant body of literature that examines the sharing of health information in online forums, or health information exchanges, the literature on the privacy aspects of PHR is still scarce.

Our work addresses this gap by looking into the intention to use PHR systems. The motivation for this research comes from the need to sustain PHR by engaging more patients with greater intensity, in an effort to improve health outcomes and reduce healthcare costs. However, across multiple studies, privacy and security concerns seem to have the most negative influence on the intentions of patients to share their private health information. On the other hand, despite the serious security and privacy concerns involved in the use of PHR, a growing body of literature argues that the widespread use of information and communication technologies in everyday life makes people more willing to accept greater privacy risks in exchange for convenience and/or better-quality health care. To sufficiently address this complex issue, we adopt the privacy calculus framework to develop a model that examines the trade-off between the perceived benefits provided through the use of PHR systems and the security risks that are associated with the use of such systems. Our model comprises richer variables for perceived risk (security beliefs) and perceived benefits that addresses the complexity that surrounds the intention to use PHR.

We collected data from 355 participants and analyzed the data using Structural Equation Modeling. Our findings show that, while individuals recognize and consider both risks and benefits related to the use of PHR, the risks weigh much more than the benefits. In fact, security beliefs lead to lower perceived benefits, as well as intention to use. Therefore, security beliefs are a strong barrier limiting individuals’ engagement in managing and sharing their personal health information and consequently preventing the success of PHR. As a result, the benefits of PHR, which include reducing costs and improving health outcomes, might not be extended.

These findings provide practical implications to healthcare providers and policy makers on how to promote PHR and engage more patients. Besides promoting PHR by highlighting their benefits, healthcare providers should also focus on addressing the risks that are relevant to security beliefs. Specifically, healthcare providers need to educate individuals on the security and privacy safeguards that are in place to protect the patients’ information. This study also provides theoretical contributions by applying the privacy calculus to the PHR context and by using richer second-order instruments to measure security beliefs and perceived benefits.

Keywords

PHR, Health IT, Privacy Calculus, Security Beliefs.