CITIZENS' HEALTH INFORMATION PRIVACY CONCERNS: A MULTIFACETED APPROACH

Research in Progress

Kenny, Grace, Dublin City University, Dublin, Ireland, grace.kenny2@mail.dcu.ie

Connolly, Regina, Dublin City University, Dublin, Ireland, regina.connolly@dcu.ie

Abstract

The increasing prevalence of ICTs in healthcare is transforming the health services received by patients. This transformation is in part facilitated by healthcare providers' utilization of eHealth technologies, which provide physicians with access to the health data required to treat patients. The recent emergence of mobile health (mHealth) technologies such as mHealth applications and personal health records (PHRs) enable citizens to play a role in this transformation by presenting them with the opportunity to manage their own health. The success of both eHealth and mHealth technologies is contingent on acceptance and adoption by both physicians and citizens. However in order to ensure success, the factors driving or inhibiting acceptance and adoption of these technologies must be understood. In the existing literature, factors driving citizen acceptance of health ICTs are under-examined. This paper focuses on citizens' health information privacy concerns (HIPC), which are regularly cited as a barrier to health ICT implementation. The paper presents a framework to investigate the influence of citizens' HIPC on their acceptance and adoption of health ICTs. An upcoming study which tests this framework and the hypotheses presented in the paper is also outlined.

Keywords: eHealth, mHealth, citizens' health information privacy concerns, HIPC.

1   Introduction

The increasing prevalence of ICTs can have transformative impacts on many industries, including healthcare where ICTs can deliver citizen centric healthcare and foster a dyadic, information symmetric, physician-patient relationship (European Commission, 2012). The shift towards citizen centric care is partly facilitated by electronic health (eHealth) technologies such as electronic health records (eHRs), which are utilized by health professionals to store, update, and share patient health data (Angst and Agarwal, 2009). Individuals are further empowered by mobile health (mHealth) technologies such as personal health records (PHRs) and mobile health (mHealth) applications, which can be utilized by citizens to self-manage chronic illnesses or monitor their general health and fitness (Eng and Lee, 2013). The implementation of eHR systems remain slow in many countries, including Ireland despite plans to introduce a national eHR (Department of Health, 2013). The European Commission's eHealth Action Plan highlights the lack of awareness and confidence in these technologies among health professionals and citizens as a barrier to growth (European Commission, 2012). Additionally, the eHealth strategy for Ireland refers to privacy as a fundamental driver of eHealth success or failure (Department of Health, 2013). It has been asserted that the biggest barrier to successful eHR adoption is achieving citizen acceptance, with information privacy representing citizens' biggest concern (Chhanabhai & Holt 2007). While numerous studies have investigated the factors driving health professionals' acceptance of eHRs (e.g. Venkatesh, Sykes, & Zhang, 2011; Walter and Lopez, 2008; Hsieh, 2014; Maillet et al., 2014), citizen acceptance has received little exploration. This is unsurprising as eHRs are predominately used by health professionals. However, the information stored in eHRs

pertains to citizens' health and many eHR systems facilitate citizen access to their health record online. Therefore, it is argued that citizens' acceptance of eHRs is important to their success and the relationship between citizens' HIPC and this acceptance warrants examination.

Due to the rise in chronic illnesses and the increasing popularity of health monitoring among healthy individuals, mHealth technologies are relevant to large masses of individuals (Fox and Duggan, 2012; 2013). The mHealth technologies of interest in this paper include; PHRs and mHealth applications. PHRs are similar to eHRs in that they allow citizens to maintain a personal digitised record of their health information. In 2010, it was estimated that approximately 7% of adults in the US used PHRs (Ackerman, 2010). Categories of mHealth applications range from diet and exercise applications to pregnancy symptom applications. In 2012, it was found that 19% of American adults used at least one mHealth application (Fox and Duggan, 2012). There are no such statistics available for the use of PHRs and mHealth applications in Europe. However, it has been estimated that over 500 million people worldwide will use a mHealth application in 2015 (Privacy Rights Clearinghouse, 2013). Research on citizens' HIPC regarding mHealth technologies is also limited. A recent study found that individuals' privacy concerns significantly reduced their intention to adopt PHRs (Li et al. 2014). This study supports the link between citizens' HIPC and their personal adoption of mHealth technologies. There are no known studies exploring citizens' HIPC regarding mHealth applications. However, HIPC has been repeatedly cited as a potential barrier to the growth of mHealth applications (Connelly et al. 2006; Järvinen, 2009; Mosa et al. 2012; Whittaker, 2012). This paper focuses on understanding citizens' HIPC and whether these concerns influence both their acceptance of eHRs - a technology introduced by health professionals, and their personal adoption of mHealth technologies. Based on a review of the existing information privacy literature, a framework for examining citizens' HIPC is presented.

2 Literature review

2.1 Information Privacy

In recent decades, there has been an explosion of information privacy research across disciplines such as Economics, Psychology, and Management Information Systems (MIS). Despite the myriad of studies, information privacy is still examined from a different lens in each discipline. For example, in Law privacy was historically defined by Warren and Brandeis (1890) as a balance between one's right to be let alone and the information needs of society. Within Psychology, privacy is defined as controlling access to information about oneself (Westin, 1967). Drawing from the understandings of these disciplines, information privacy is defined in MIS as an individual's desire to have greater control over the collection and dissemination of their information (Bélanger and Crossler, 2011). Unlike Westin's definition, this definition does not imply that individuals have control over the information they disclose, but that they desire greater control. In this paper, information privacy is described as citizens' desire to be afforded greater control over the collection and dissemination of their personal health information.

2.2 Examining Information Privacy

The disparities in information privacy research extend beyond definitions to approaches used to investigate the construct. Despite the plethora of existing studies, calls to exercise comprehensive, multidisciplinary approaches when examining information privacy remain largely unanswered (Phelps, Nowak and Farrell, 2000; Smith et al. 2011). It can be argued that it may not be possible to develop an all-encompassing, repeatable framework for investigating information privacy across every context. Nonetheless, the information privacy literature would benefit from studies that whilst considering the context-specific factors that could potentially be influential, simultaneously follow a comprehensive

approach. Upon conducting an interdisciplinary review of the information privacy literature, Smith et al. (2011) called for future information privacy studies to adopt a comprehensive approach. They presented the Antecedents → Privacy Concerns → Outcome macro model (APCO) as a broad guide for future studies. Under APCO, information privacy is examined by exploring the drivers of concern, the dimensions of privacy concern and the outcome of concern.

2.3   Information Privacy in Health Informatics

In the Health Informatics literature, the need to address information privacy prior to eHR implementation has been stressed (Rothstein, 2007). A number of studies have found that citizens consistently express high privacy concerns regarding their health data (Chhanabhai, and Holt, 2007; Goodwin et al. 2002; Flynn et al. 2002). The existing literature in this domain examining information privacy and eHRs illustrates the relevance of information privacy. However, there are some notable weaknesses in the approach used to examine information privacy. For example, a systematic review of studies examining information privacy and eHRs revealed that all 21 studies failed to adequately distinguish between privacy and security concerns (Shaw et al. 2011). While security relates to the *technical measures* in place to protect data in eHRs (King et al. 2012), privacy pertains to *individuals' desire to control* the use of this data. This weakness obfuscates our understanding of the role of privacy in this context. Another related weakness is the examination of information privacy concerns as a one-dimensional construct, often using a single item. This approach contrasts with the considerable evidence supporting the multidimensionality of the information privacy construct (Hong and Thong, 2013) and fails to provide insight into the interrelationships between the dimensions of information privacy concern and antecedents or outcomes.

Due to the nascence of mHealth technologies, citizens' HIPC have received limited attention in the literature. As noted, Li et al. (2014) found that HIPC significantly reduced citizens' intention to adopt PHRs. The authors called for future research to investigate privacy and mHealth technologies. A systematic review of studies examining mHealth applications yielded 14 patient focused studies, all of which focused on usability and health outcomes associated with the applications as opposed to privacy, but the authors of the review stressed the need for future research to examine citizens' HIPC (Mosa et al. 2012). This assertion is shared by others (Connelly et al. 2006; Whittaker, 2012). It can be argued that existing mHealth applications fail to address privacy, as a study of 600 mHealth applications found that none on these applications informed users of how their data was used (Eng and Lee, 2013). Due to the weaknesses inherent in information privacy studies regarding eHRs and the paucity of studies centred on different mHealth technologies, future research can greatly improve our limited understanding of the role information privacy plays in this context.

3   HIPC Framework

In line with the need for comprehensive studies, this paper follows the APCO framework to develop the approach to examine citizens' health information privacy concerns and how they influence acceptance and adoption of health ICTs outlined below in Figure 1. Additional support for the examination of Antecedents → Privacy Concerns → Outcomes is provided by the Theory of Reasoned Action (TRA) which posits that human behavioural decisions are explained as follows: Beliefs→ Attitudes→ Intention→ Actual Behaviour (Azjen and Fishbein, 1977). Based on TRA, antecedents on the left of the framework below refer to individuals' beliefs and perceptions that are likely to influence their HIPC. In the centre, HIPC or attitudes in TRA are described as individuals' concerns regarding the collection, use and dissemination of their personal health information by different healthcare entities (Angst and Agarwal, 2009). On the right, outcomes or intention in TRA relate to individuals' acceptance of eHRs and intention to adopt mHealth technologies. The reasoning behind the inclusion of each of the factors in the framework is discussed in the following sections.
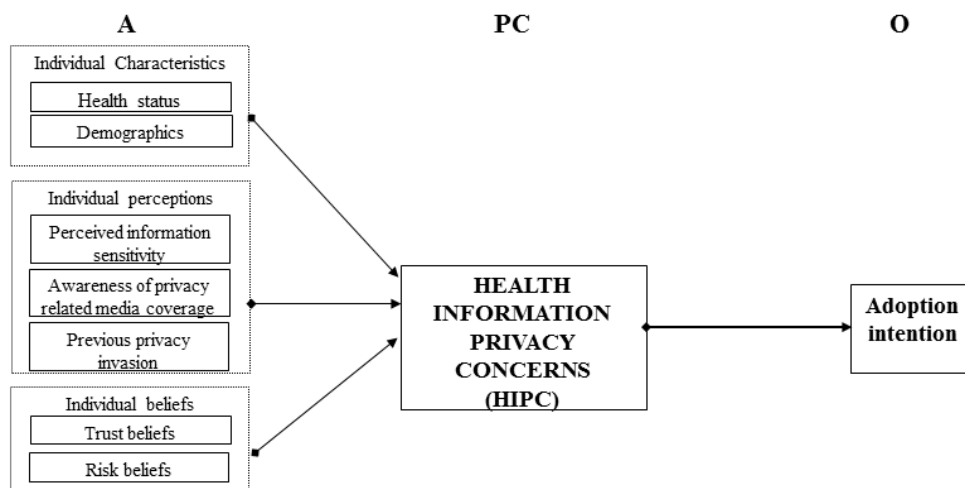
Figure 1.   Research Framework for examining citizens' HIPC

4   Antecedents

The information privacy literature is replete with studies examining context-specific antecedents. Following an extensive review of the literature, Li (2011) categorized all antecedents. Based on Li's work and a review of the health informatics literature, a number of potential antecedents to citizens' HIPC are presented. It is acknowledged that this list may not be comprehensive, but it provides an initial attempt to encompass both information privacy and health informatics literature regarding antecedents.

4.1   Individual Characteristics

Few studies have explored demographic variables in the context of citizens' HIPC. However, in the existing literature both gender and age have been shown to exert an influence. With regards to age, older individuals have been found to express higher privacy concerns (King et al. 2012; Laric et al. 2009). Females have also been found to express higher concerns regarding their health data (Laric et al. 2009). On the basis of these findings, the following hypotheses are proposed:

H1: Age will positively impact HIPC.

H2: Females will express higher HIPC than males.

Additional demographic variables such as education and income have been examined in other privacy contexts with mixed results. Education was found to have an insignificant influence on individuals' personal information privacy concerns by Zhang et al. (2002) and Chen et al. (2001), but was significant in a study by Phelps, Nowak and Farrell (2000) who found that college graduates expressed the lowest level of concern. Similarly, income was insignificant in two studies (Phelps, Nowak and Farrell 2000; Chen et al. 2001). However, one study found that income was insignificant among US respondents but significant among Chinese respondents (Zhang et al. 2002). The role of education and income on HIPC can be tested. However, no specific hypotheses are presented at this time.

Many argue that health status influences individuals' HIPC. However, the direction and nature of this influence is uncertain. Some argue that individuals with health conditions will be less concerned about privacy, due to the benefits they can gain from physician and personal use of health ICTs (Angst & Agarwal, 2009). In support of this, a recent study found that respondents with chronic illnesses are more willing to share health data (Lafky and Horan, 2011). Some findings refute this argument, showing that certain illnesses, especially those surrounded by stigma such as HIV, increase HIPC (Flynn et

al. 2003; van Heerden et al. 2013). Therefore, it is argued that chronic illnesses and sensitive illnesses will influence HIPC in different ways. To test this assertion, the following hypothesis is proposed:

H3: Individuals with chronic conditions will express lower HIPC than those with sensitive conditions.

Individuals with sensitive health conditions such as HIV or mental health conditions may have experienced stigmatization or negative differential treatment in the past. It can be argued that previous stigmatization due to health condition will increase individuals' privacy concern regarding this information. While this has not yet been examined, calls have been made for future studies to investigate the influence of stigmatization (Shaw et al. 2011). Thus the following hypothesis is proposed:

H4: Experience of past stigmatization due to health condition will be positively related to HIPC.

4.2   Individual Perceptions

This section discusses a number of possible antecedents related to individuals' perceptions of knowledge, sensitivity, and personal experience. The first is perceived sensitivity of health information. It has been found that the perception of how sensitive different types of information are varies from one individual to another. For example, a recent study found that individuals were less willing to share information in eHRs that they deemed sensitive. This included information pertaining to genetics, mental health, reproductive health, and substance abuse (Caine and Hanania, 2013). With regards to the relationship between perceived information sensitivity and HIPC, Bansal et al. (2010) found that perceived information sensitivity increased individuals' HIPC. It is thus hypothesised:

H5: Perception of health information sensitivity will positively influence HIPC.

Awareness of privacy related media coverage has been found to impact individuals' information privacy concerns (Smith et al. 1996). This is relevant due to the volume of media coverage surrounding health ICTs and privacy. For example, eHR implementation in England was met with heavy media criticism regarding privacy, this impacted implementation in Wales where a comprehensive eHR was rejected and replaced with a summary record (Greenhalgh et al. 2012). It is thus argued that individuals who are aware of media coverage regarding privacy issues and health information will be more concerned for the privacy of their personal health data. The following hypothesis tests this assertion:

H6: Awareness of health privacy related media coverage will positively influence HIPC.

It is claimed that individuals who perceive they have experienced past privacy breaches are more likely to express higher information privacy concerns. This assertion has been widely supported across contexts including health, with a recent study finding past privacy breaches significantly increased health information privacy concern (Bansal et al. 2010). Thus it is hypothesized:

H7: Experience of previous privacy breaches will positively impact HIPC.

4.3   Individual Beliefs

There are a number of individual beliefs that may impact HIPC. The first relates to individuals' trust beliefs which have been found to reduce information privacy concern in a number of contexts. In the context of internet privacy concerns, Hong and Thong (2013) found that trust in technology vendors had a negative impact on individuals' information privacy concern. The relationship between trust and privacy concern has not been explored in the context of citizens' HIPC. Based on the findings of other contexts, the following hypothesis is presented:

H8a: Trust in health technology vendors will have a negative influence on HIPC.

In addition to health technology vendors, it is argued that trust in health professionals is of the utmost importance in this context. Despite a lack of empirical investigation, Rahim et al. (2013) assert that trust in health professionals would reduce privacy concerns. The following hypothesis is presented:

H8b: Trust in health professionals will have a negative influence on HIPC.

Risk beliefs relate to individuals' beliefs regarding the risks associated with providing a certain party with their personal information. Risk beliefs have been found to increase information privacy concerns in internet-based contexts (Hong and Thong, 2013; Malhotra et al. 2004), but are yet to be examined in terms of their influence on HIPC. Similar to the role of trust beliefs, risk can be discussed in terms of the risks associated with providing health information to health technology vendors and to health professionals. Based on the role of risk in other contexts, the following hypotheses are presented:

H9a: Risk beliefs associated with health technology vendors will positively impact HIPC.

H9b: Risk beliefs associated with health professionals will positively impact HIPC.

Trust beliefs have been found to reduce risk beliefs in various contexts including health, with a recent study finding trust in health technology vendors reduced risk beliefs associated with these vendors (Li et al. 2014). To test the relation between trust and risk, the following hypotheses are presented:

H10a: Trust in health technology vendors will have a negative influence on risk beliefs regarding these vendors.

H10b: Trust in health professionals will have a negative influence on risk beliefs regarding health professionals.

5 Information Privacy Concerns

The central component of the APCO framework is information privacy concerns. As noted, privacy concern is rarely measured in Health Informatics using a validated measure. However the innumerable information privacy studies in other disciplines has led to the emergence of a large number of privacy concern measures. Among these measures there is a high degree of overlap in terms of dimensions measured. The most popular dimensions examined in past literature are collection, unauthorized secondary use, improper access, errors, control, and awareness (Hong and Thong, 2013). Each dimension is now outlined in terms of its relevance to privacy in the health context.

5.1 Collection

The collection dimension relates to individuals' concern regarding an organization's collection and storage of a great deal of their personal information (Smith et al. 1996). In the context of health information, collection relates to an individual's concern regarding the collection and storage of health information by healthcare entities (Angst and Agarwal, 2009). Due to the sensitive nature of health information, it can be posited that individuals will be concerned by the collection of large volumes of their health data and the permanency of storing this data in health ICTs.

5.2 Unauthorized Secondary Use

Unauthorized secondary use of one's information occurs when information is collected for one purpose and subsequently used for a secondary purpose without obtaining permission (Smith et al. 1996). There are many uses for health data such as diagnosing patients, treating patients, conducting health research, and non-health related purposes such as marketing and media usage (Järvinen, 2009). It is also highlighted that individuals aren't aware of how many organizations view their health data (Angst, 2006). For example, organizations with access to data in mHealth applications include wire-

less carriers, phone manufacturers, and application developers (Eng and Lee, 2013). Due to the number of parties accessing health data and the myriad of potential uses, it is argued that unauthorized secondary use is relevant to examining citizens' HIPC.

5.3   Improper Access

This dimension relates to individuals' concern that an organization does not have the measures in place to prevent unauthorized individuals from accessing their personal information (Smith et al. 1996). Numerous studies have found that citizens are worried about improper access to their health information by hackers (Chhanabhai and Holt, 2007), malicious employees (Powell et al. 2007), legal and insurance companies (Pyper et al. 2008). Furthermore, individuals express high levels of concern regarding the repercussions of improper access, such as possible stigmatization (Flynn et al. 2003). It is thus argued that individuals will express concerns regarding improper access to their health data.

5.4   Errors

The errors dimension relates to individuals' concern that an organization does not have the measures in place to prevent against errors in the data (Smith et al. 1996). Approximately 65% of respondents in a US study believed that digitizing health data would result in more errors (Westin, 2005). In another study, 32% of individuals found errors in their health data stored in eHRs (Powell et al. 2007). It is thus argued that individuals will express concerns over potential errors in their health data.

5.5   Control

This dimension relates to individuals' concern regarding the lack of control they have over their data (Malhotra et al. 2004). Individuals value control, as shown in a recent study with all respondents expressing a desire to control what health professionals could access what health data (Caine and Hanania, 2013). Furthermore when eHR systems don't offer individuals some control, they express higher privacy concerns (Li and Slee, 2014). Thus, it is argued if individuals feel they lack control over their health data in eHRs and mHealth technologies, they will express higher HIPC.

5.6   Awareness

This dimension relates to an individual's concern regarding their lack of awareness of how an organization uses and protects the privacy of their data (Malhotra et al. 2004). The lack of awareness patients have regarding how their health data is used has been repeatedly highlighted (Angst, 2006; Goodwin et al. 2002). The link between this lack of awareness and privacy concern was shown in a study where a large majority of respondents were unaware that their health data was stored in eHRs and when they were informed expressed high privacy concerns (Chhanabhai and Holt, 2007). Thus, it is argued that awareness is relevant to examining citizens' health information privacy concerns.

5.7   Measuring HIPC

Based on this discussion, it is argued that these six dimensions are relevant to examining citizens' HIPC. The Internet Privacy Concern measure (IPC) was developed by Hong and Thong in 2013 based on the two most popular measures of privacy concern; Concern for Information Privacy (CFIP) and Internet Users' Information Privacy Concerns (IUIPC). The IPC measure consists of a third-order general factor representing privacy concern, two second-order factors of interaction management, and information management, and six first-order factors (the dimensions discussed above) (Hong and Thong, 2013). While the IPC has not yet been applied to the health context, four of the six first-order factors

(collection, unauthorized secondary use, improper access and errors) were successfully applied to a study of privacy concern regarding eHRs (Angst and Agarwal, 2009). The relevance of the two remaining dimensions of awareness and control is argued in this paper. Further support for the use of the IPC in this context is offered due to its applicability to specific contexts within a nomological model to examine all elements of information privacy (Hong and Thong, 2013). It is thus argued that IPC is an appropriate measure to examine citizens' HIPC within the APCO framework.

6   Outcomes

In order to illustrate the importance of understanding privacy, the outcomes of information privacy concerns must be measured. This paper focuses on the influence of HIPC on two outcomes related to technology adoption. The first relates to citizens' acceptance of eHRs introduced by health professionals, and the second relates to individuals' intention to adopt mHealth technologies such as PHRs and mHealth applications. These outcomes can be examined using a validated technology adoption model. To date, the Unified Theory of Acceptance and Use of Technology (UTAUT) and Technology Acceptance Model (TAM) have been applied in a small number of studies examining citizens' acceptance of various health ICTs (Bidmon et al. 2014; Hennington, and Janz, 2007; Klein, 2007). None of these studies focused on privacy, but calls have been made to utilize technology adoption models when investigating the impact of privacy on the adoption of health ICTs (Angst and Agarwal, 2009). Additionally, studies have shown that HIPC negatively impacts intention to use PHRs and participate in virtual health communities; although neither of these studies utilized a validated technology adoption model (Li et al. 2014; Kordzadeh and Warren, 2014). While deciding on the appropriate technology adoption model is beyond the scope of this paper, the following broad hypotheses are presented:

H11a: HIPC will negatively impact individuals' acceptance of eHRs.

H11b: HIPC will negatively influence individuals' intention to adopt mHealth technologies.

7   Methodology: Testing the HIPC Framework

The framework for examining citizens' HIPC presented in Figure 1 will be tested in an upcoming Irish study. The first stage of the study will be a survey. To explore the relationships hypothesised in this paper, the IPC measure will be adapted to examine health information privacy concern. The impact of each antecedent outlined in this paper on the third-order general factor of HIPC will be investigated. Lastly the influence of citizens' HIPC on their acceptance of eHRs and their intention to use mHealth technologies will be examined. Due to the embryonic nature of this research area, follow-up interviews will also be conducted. These interviews aim to: gain a greater understanding of the dimensions of HIPC, achieve a deeper insight into antecedents, identify any possible additional antecedents, delve further into the relationship between HIPC and citizens' acceptance and adoption of health ICTs, and identify any conditions individuals might express prior to accepting or adopting these technologies.

8   Conclusion

It is widely accepted that both eHRs and mHealth technologies have great potential to advance healthcare. However, citizens' HIPC represent a barrier to the successful implementation of these technologies. Our knowledge of the role of citizens' HIPC is extremely limited at present, due predominately to a lack of comprehensive studies. This paper introduces a citizen-centric approach to examine the role of HIPC, by presenting a framework to study the antecedents, privacy concerns, and outcomes. It is acknowledged that other factors may be influential, but it is maintained that the framework presented above represents a strong starting point. The results from this study can contribute to our understanding of citizens' HIPC and identify possible avenues for future research.

References

Ackerman, K. (2010). *Survey Finds Benefits of PHR Use, But Adoption Remains Low.* URL: http://www.ihealthbeat.org/insight/2010/survey-finds-benefits-of-phr-use-but-adoption-remains-low (visited on 12/01/2014)

Ajzen, I., and Fishbein, M. (1977). "Attitude-behavior relations: A theoretical analysis and review of empirical research." *Psychological Bulletin*, 84(5), 888–918.

Angst, C. M. (2006). "Protect My Privacy or Support the Common-Good? Ethical Questions about Electronic Health Information Exchanges." *Journal of Business Ethics*, 90(2), 169–178.

Angst, C. M. and R. Agarwal (2009). "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion." *MIS Quarterly,* 33(2), 339–370.

Bansal, G. Zahedi, F. M. and D. Gefen (2010). "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online." *Decision Support Systems,* 49(2), 138–150.

Bélanger, F. and R. E. Crossler (2011). "Privacy in the digital age: a review of Information privacy research in Information systems." *MIS Quarterly,* 45(4), 1017–1041.

Bidmon, S. Terlutter, R. and J. Röttl (2014). "What explains usage of mobile physician-rating apps? Results from a web-based questionnaire." *Journal of Medical Internet Research,* 16(6), e148.

Caine, K. and R. Hanania (2013). "Patients want granular privacy control over health information in electronic medical records." *Journal of the American Medical Informatics Association: JAMIA,* 20(1), 7–15.

Chen, J., Zhang, Y., and Heath, R. (2001). "An Exploratory Investigation of the Relationships Between Consumer Characteristics and Information Privacy." *Marketing Management Journal,* 11(1), 73–81.

Chhanabhai, P. and A. Holt (2007). "Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures." *Medscape general medicine,* 9(1), 8.

Connelly, K. H. Faber, A. M. Rogers, Y. Siek, K. A. and T. Toscos (2006) "Mobile applications that empower people to monitor their personal health." *e & i Elektrotechnik und Informationstechnik,* 123(4), 124–128.

Department of Health (2013). *eHealth Strategy for Ireland.* URL: http://health.gov.ie/wp-content/uploads/2014/03/Ireland_eHealth_Strategy.pdf (visited on 02/12/2014)

Eng, D. S. and J. M. Lee (2013). "The promise and peril of mobile health applications for diabetes and endocrinology," *Pediatric diabetes,* 14(4), 231–8.

European Commission. (2012). *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century.* URL: http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf (visited on 12/12/2014)

Flynn, H. Marcus, S. Kerber, K. and N. Alessi (2003). "Patients' concerns about and perceptions of electronic psychiatric records." *Psychiatric Services,* 54(11), 1539–1541.

Fox, S. and M. Duggan (2012). *Mobile Health.* URL: http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobileHealth2012_FINAL.pdf (visited on 09/02/2014).

Fox, S. and M. Duggan (2013). *Tracking for Health.* URL: http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_TrackingforHealth%20with%20appendix.pdf (visited on 09/02/2014).

Goodwin, L. Courtney, K. Kirby, D. and M. A. Iannacchione (2002). "A pilot study: Patients' perceptions about the privacy of their medical records." *Online Journal of Nursing Informatics,* 6(3)

Greenhalgh, T. Morris, L. Wyatt, J. C. Gwyn, T and K. Gunning (2013). "Introducing a nationally shared electronic patient record : Case study comparison of Scotland, England, Wales and Northern Ireland." *International Journal of Medical Informatics,* 82, 125–138.

Hennington, H. and B. D. Janz (2007). "Information systems and Healthcare XVI: Physician Adoption of Electronic Medical Records: Applying the UTAUT model in a Healthcare context." *Communications of the Association for Information Systems,* 19, 60–80

Hong, W. and J. Thong (2013). "Internet Privacy Concerns: an Integrated Conceptualisation and four empirical studies." *MIS Quarterly,* 37(1), 275–298.

Hsieh, P.-J. (2014). "Physicians' acceptance of electronic medical records exchange: An extension of the decomposed TPB model with institutional trust and perceived risk." *International Journal of Medical Informatics,* 1–14.

Järvinen, O.P. (2009). "Privacy Management of Patient-Centered E-Health", In: *Patient-Centered E-Health,* E.V Wilson, Ed. p. 81-97. Hershey: PA IGI Global.

King, T. Brankovic L. and P. Gillard (2012). "Perspectives of Australian adults about protecting the privacy of their health Information in statistical databases." *International Journal of Medical Informatics,* 81(4), 279–89.

Klein, R. (2007). "Internet-Based Patient-Physician Electronic Communication Applications: Patient Acceptance and Trust." *e-Service Journal*, 5(2), 27–52.

Kordzadeh, N. and J. Warren (2014). "Current health status: Personal Characteristics, Privacy Concern, and Membership in Virtual Health Communities: An Empirical Study." In: *Proceedings of the Twentieth Americas Conference on Information Systems,* Savannah, p.1–10.

Lafky, D.B. and T. A. Horan (2011). "Personal health records: Consumer attitudes toward privacy and security of their personal health information." *Health Informatics Journal,* 17(1), 63–71.

Laric, M. V. Pitta, D. A. and L. P. Katsanis (2009). "Consumer Concerns for Healthcare Information Privacy: A comparison of US and Canadian Perspectives." *Research in Healthcare Financial Management,* 12(1), 93–111.

Li, H., Gupta, A., Zhang, J., and Sarathy, R. (2014). "Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract." *Decision Support Systems,* 57(2014), 376–386.

Li, T. and T. Slee (2014). "The effects of information privacy concerns on digitizing personal health records." *Journal of the Association for Information Science and Technology*, 65(8), 1541–1554.

Li, Y. (2011). "Empirical Studies on Online Information Privacy Concerns : Literature Review and an Integrative Framework." *Communications of the Association for Information Systems,* 28(28), 453–496.

Maillet, E., Mathieu, L., and Sicotte, C. (2014). "Modeling factors explaining the acceptance, actual use and satisfaction of nurses using an Electronic Patient Record in acute care settings: An extension of the UTAUT." *International Journal of Medical Informatics,* 1–12.

Malhotra, N. K. Kim, S. S. and J. Agarwal (2004). "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale and a Causal Model." *Information Systems Research,* 15(4), 336–355.

Mosa, S. M. Yoo, I. and L. Sheets (2012). *"*A systematic review of healthcare applications for smartphones." *BMC medical informatics and decision making,* 12(67), 1–31.

Phelps, J. E. Nowak, G. and E. Farrell (2000). "Privacy Concerns and Consumer Willingness to Provide Personal Information." *American Marketing Association,* 19(1), 27–41.

Powell, J. Fitton, R. and C. Fitton, "Sharing electronic health records: the patient view." *Informatics in primary care,* 14(1), 55–7.

Privacy Rights Clearinghouse. (2013). *Mobile Health and Fitness Apps: What Are the Privacy Risks?* URL: https://www.privacyrights.org/mobile-medical-apps-privacy-alert (visited on 30/11/2014)

Pyper, J. Amery, M. Watson and C. Crook (2008). "Patients' experiences when accessing their on-line electronic patient records in primary care." *British Journal of General Practice,* 54(498), 38–43.

Rahim, A. Ismail, Z. and G. N. Samy (2013). "Information Privacy Concerns in Electronic Healthcare Records : A Systematic Literature Review." In: *Proceedings of the 3rd International Conference on Research and Innovation in Information Systems – 2013 (ICRIIS'13*), Kuala Lumpur, 504–509.

Rothstein, M. A. (2007). "Health privacy in the electronic age." *The Journal of Legal Medicine,* 28(4), 487–501.

Shaw, N. T. Kulkarni, A. and R. L. Mador (2011). "Patients and Health Care Providers' Concerns about the Privacy of Electronic Health Records: A Review of the Literature." *Electronic Journal of Health Informatics,* 6(1), 1–5.

Smith, H.J. Dinev, T. and H. Xu (2011). "Information privacy research: an Interdisciplinary review." *MIS Quarterly,* 35(4), 989–1015.

Smith, H.J. Milberg, S. J. and S. J. Burke (1996). "Information privacy: Measuring individuals concerns about organizational practices." *MIS Quarterly,* 20, 167–196.

van Heerden, A. Norris, S. Tollman, S. Richter, L. and M.J. Rotheram-Borus (2013). "Collecting maternal health information from HIV-positive pregnant women using mobile phone-assisted face-to-face interviews in Southern Africa." *Journal of Medical Internet Research,* 15(6), e116.

Venkatesh, V., Sykes, T., and Zhang, X. (2011). "Just what the doctor Ordered: A Revised UTAUT for EMR System Adoption and Use by Doctors." In: *Proceedings of the 44th Hawaii International Conference on System Sciences,* Hawaii, 1–10.

Walter, Z., and Lopez, M. S. (2008). "Physician acceptance of information technologies: Role of perceived threat to professional autonomy." *Decision Support Systems*, 46(1), 206–215.

Warren, S. and L. Brandeis (1890). "The Right to Privacy." *Harvard Law Review,* 193-220.

Westin, A. (1967). *Privacy and Freedom*. New York: Athenbaum,

Westin, A. (2005). "Public Attitudes toward Electronic Health Records." *Privacy and American Business,* 12(2), 2–6.

Whittaker, R. (2012). "Key Issues in Mobile Health and Implications for New Zealand." *Healthcare and Informatics Review Online,* 16(2), 2–7.

Zhang, Y., Chen, J. and Wen, K. W. (2002). "Characteristics of Internet Users and Their Privacy Concerns—A Comparative Study Between China and the United States." *Journal of Internet Commerce,* 1(2), 1–16.