Examining Citizens’ Health Information Privacy Concerns: An Extension of the IPC Instrument

Completed Research Paper

Grace Kenny
Irish Centre for Cloud Computing and Commerce (IC4),
Dublin City University
grace.kenny@dcu.ie

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

Abstract
The increasing social emphasis on wellness empowers individuals to track and manage their personal health using mobile health applications and wearable tracking devices. However, these devices require the disclosure and generation of copious amounts of sensitive health data and thus often foster concerns regarding the privacy of individuals’ health data. Notwithstanding that fact, the few studies that have examined citizens’ information privacy concerns in the health context focus either on a specific technology or utilize a one-dimensional measure of concern. In order to develop a deeper understanding of citizens’ health privacy concerns, this replication study adapts the six-dimensional Internet Privacy Concerns instrument to empirically test citizens’ health privacy concerns in the United States and Ireland. The paper advances understanding by illustrating the applicability of this measure in the complex health context, and elucidating how citizens’ health privacy concerns reduce trust and heighten risk perceptions associated with health technology vendors.

Keywords
Health information privacy concerns, information privacy concerns, replication research.

Introduction
Information privacy has garnered increasing interest in the form of public discourse, policy refinements and empirical research across various contexts. However, only a small number of studies have examined information privacy within the sensitive context of health, a fraction of which have focused on citizens. The under-examination of privacy in this context is worrying as health is an issue of fundamental importance to society and individuals, and privacy issues remain contentious in this context (Payton et al. 2011). Furthermore, privacy has represented one of the fundamental building blocks of healthcare delivery for centuries, with doctors around the world pledging to protect patients’ privacy under the Hippocratic Oath. Thus, the changing role of privacy brought about by technical advancements and societal changes remains relatively unknown. It is argued that the health context represents a fruitful avenue for information privacy research for four reasons. Firstly, due to its personal nature, health information is widely viewed as more sensitive or personal than other information types. For instance, 93% of Irish citizens describe their health information as very sensitive or the information they most desire to keep private (Eurobarameter, 2011). Secondly, individuals have been found to express high privacy concerns regarding their health data (Lakfy and Horan, 2011). Thirdly, if health data privacy is not protected, individuals’ lives can be negatively impacted (Anderson and Agarwal, 2011). Fourthly, health information privacy concerns (HIPC) reduce individuals' willingness to adopt health technologies (Angst and Agarwal, 2009), and cause individuals to withhold health data (Campos-Castillo and Anthony, 2014). These behaviors are particularly important in the health context as withholding health data from health professionals or health technologies can lead to dangerous misdiagnoses, reduce the quality of care received or damage the health recommendations provided by mobile health technologies. Recent studies on health information privacy (Angst and Agarwal, 2009; Dinev et al., 2016) illustrate both the relevance
of this research stream and the negative influence of citizens’ health information privacy concerns on their attitudes and intentions towards health technologies such as Electronic Health Records (EHRs). Due to the nascence of this stream of research, many gaps persist in our understanding of privacy in the health context, thus supporting the need for further exploration. Two core gaps include the tendency of prior work to focus on privacy concerns regarding one specific health technology and the lack of agreement surrounding the measurement of privacy concerns in the health context. This study aims to address these gaps by focusing on citizens’ privacy concerns regarding personal health information which may be collected by health organizations or technology companies. Specifically, the study seeks to capture citizens’ concerns regarding the storage, dissemination, and use of the personal health information they disclose to health organizations or mobile health technologies. To this end, the study adapts the six-dimensional Internet Privacy Concerns measure. We argue that through replicating the most comprehensive existing measure and extending it to the health context, this study can provide some much needed clarity in the health information privacy domain. Retesting and validating this measure represents a requisite step to addressing privacy and negating the negative outcomes associated with concern.

The paper proceeds with a discussion on the popular constructs used to examine privacy concerns prior to focusing on measures within the health context. The methodology followed is outlined. Findings from surveys in two countries are then detailed. The paper concludes with a brief discussion on how these findings advance our understanding of information privacy in the health context.

**Literature Review**

It is often argued that a universally accepted, conceptualization of information privacy cannot be attained, due to the varying perspectives from which it is examined (Pavlou, 2011). This paper intersects the disciplines of Information Systems (IS) and Health Informatics (HI). Within the IS field, a leading conceptualization is provided by Bélanger and Crossler (2011) who build on the assertions of Clarke (1999) to define privacy as an individual’s desire to control how their personal information is collected and disseminated. In contrast, most HI studies do not offer a definition of privacy nor do they adapt an existing definition. Furthermore, many of these studies fail to adequately differentiate privacy from similar but distinct concepts such as confidentiality or the sharing of information with select individuals, and security which refers to the technical measures in place to secure data (Shaw et al., 2011). This paper thus adapts the definition provided by Bélanger and Crossler (2011) describing privacy as an individual’s desire for greater control over the collection, use, and dissemination of their personal health information by health organizations and health technology vendors (Kenny and Connolly, 2015). The emphasis in this context is on greater control not complete control, as data disclosure is required to receive treatment from health professionals or to engage in personal health tracking using mobile health technologies.

**Measuring Privacy**

It is important at the outset to establish what is meant by privacy concerns. Angst and Agarwal (2009) describe privacy concern as individuals’ concerns regarding the collection, use and dissemination of their health information by health entities. Building upon this definition, health information privacy concerns are described here as individuals’ concerns regarding the collection, use, and dissemination of their personal health information by different health entities and technology vendors. The definitional fragmentation that characterizes privacy definitions is equally reflected in its operationalization. Across the existing measures of concern, there is no agreed upon set of dimensions or factor structure for empirically measuring concern (Hong and Thong, 2013). However, whilst each existing measure is comprised of a different number of dimensions, and differs in the naming of dimensions, some similarities are evident. Bélanger and Crossler (2011) describe the dominant measures of privacy concern as Concern for Information Privacy or CFIP, developed to measure individuals’ concerns of how organizations use their information (Smith et al., 1996) and Internet Users’ Information Privacy Concerns or IUIPC which measures privacy concerns in the online environment (Malhotra et al., 2004). CFIP is comprised of four dimensions; collection, unauthorized secondary use, improper access, and errors. CFIP has been applied in a larger number of studies and contexts (Bélanger and Crossler; 2011). IUIPC is formed from three dimensions; collection, control, and awareness. The six dimensions which form CFIP and IUIPC are the most popular dimensions in the existing literature (Hong and Thong, 2013).
In 2013, Hong and Thong combined CFIP and IUIPC to develop the six-dimensional Internet Privacy Concerns (IPC) measure. To date, only CFIP has been used in health privacy studies (Angst and Agarwal, 2009; Li and Slee, 2014). While this supports the relevance of the CFIP dimensions, the authors of the acknowledged the importance of routine re-examination of the measure, to ascertain its continued relevance in light of advances in research and technology (Smith et al., 1996). Furthermore, researchers have called for the examination of IUIPC dimensions such as ‘Control’ in the health context (Kordzadeh et al., 2016). Table 1 below illustrates the relevance of each dimension. It is concluded that IPC represents the most appropriate measure. It is termed the Health Information Privacy Concerns (HIPC) measure.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Original Definition</th>
<th>Relevance to Health Context</th>
<th>HIPC Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection (CFIP &amp; IUIPC)</td>
<td>Individuals’ concern that an organization is collecting and storing a great deal of their personal information (Smith et al. 1996).</td>
<td>The growing prevalence of digital data storage by health organizations coupled with the emergence of mobile health solutions results in the generation and storage of copious volumes of personal health data.</td>
<td>Individuals’ concern regarding the collection and storage of large quantities of health data by health entities and technology vendors.</td>
</tr>
<tr>
<td>Unauthorized Secondary Use (CFIP)</td>
<td>Concern that data is collected for one purpose and used for a secondary purpose without permission (Smith et al., 1996).</td>
<td>Health data has many potential uses for health and technology organizations. Existing research shows that mobile health applications use and share data in many ways which may conflict with individuals’ desire to keep this data private (FTC, 2014).</td>
<td>Concern that health information collected for one purpose, is used for another without the individual’s permission.</td>
</tr>
<tr>
<td>Improper Access (CFIP)</td>
<td>Concern that an organization does not have the measures in place to protect against unauthorized individuals accessing personal information (Smith et al. 1996).</td>
<td>The many data breaches dominating international news and the findings of studies suggest that health data is not protected against misuse and intrusion.</td>
<td>Individuals’ concern that unauthorized individuals might access their personal health data.</td>
</tr>
<tr>
<td>Errors (CFIP)</td>
<td>Concern that the organization does not have the measures in place to prevent errors in personal data (Smith et al. 1996).</td>
<td>Errors in health data may result in adverse treatment and health outcomes for the individual, which are likely to cause concern.</td>
<td>Concern that health and technology organizations do not have the measures in place to prevent and correct errors in health data.</td>
</tr>
<tr>
<td>Control (IUIPC)</td>
<td>Individuals’ concerns regarding their lack of control over their data (Malhotra et al. 2004).</td>
<td>Perceived control can reduce individuals’ health privacy concerns (Dinev et al. 2016). Likewise, if individuals perceive they have no control, they are likely to express concerns.</td>
<td>Individuals’ concern that they cannot exercise control over their personal health data.</td>
</tr>
<tr>
<td>Awareness (IUIPC)</td>
<td>Individuals’ concerns regarding their lack of awareness of how an organization uses and protects the privacy of their personal information (Malhotra et al. 2004).</td>
<td>Individuals often lack awareness of how their health data is stored and used. This lack of awareness can manifest in high privacy concerns (Chhanabhai and Holt, 2007).</td>
<td>Individuals’ concern that they lack awareness of how their health data is used and protected.</td>
</tr>
</tbody>
</table>

Table 1. Dimensions of Concern

Proposed Model

In line with the model tested by Hong and Thong (2013), this study explores the relationship between citizens’ HIPC and their trust and risk perceptions. Firstly, studies (Malhotra et al., 2004; Hong and Thong, 2013) have shown that high privacy concerns reduce trust in online organizations. In the health context, the role of trust remains less clear. For example, while trust in Electronic Health Record vendors has been found to reduce concerns (Dinev et al., 2016), privacy concerns regarding health websites did not significantly impact trust in these websites (Bansal et al., 2010). Furthermore, the relationship between HIPC and trust in technology vendors such as mobile health application vendors has not yet been
examined and requires further investigation (Li, 2011). In line with findings in other contexts, this study argues that HIPC will negatively impact citizens’ trust perceptions regarding health technology vendors. Secondly, risk perceptions or individuals’ expectation that disclosing health information to a particular organization will result in a negative outcome (Featherman and Pavlou, 2003; Dinev et al., 2012). Studies in the Internet context support the positive association between perceived risks and information privacy concerns (Malhotra et al., 2004; Hong and Thong, 2013). However, the direct relationship between HIPC and risk perceptions remains unexplored. Following findings in other contexts, it is posited that HIPC will positively impact risk perceptions related to health technology vendors.

**Methodology**

This paper is classified as a conceptual replication (Dennis and Valacich, 2014) as it retests the IPC measure and the relationships between HIPC, trust, and risk in the new context of health. The study adopts a two-stage sequential mixed methods approach to develop an in-depth understanding of the HIPC phenomenon (Venkatesh, Brown, and Bala, 2013). The first stage is an exploratory pre-study that tests the relevance of the measure. The second stage is explanatory and empirically tests the instrument and the relationships of interest.

**Exploratory Interviews**

Six exploratory interviews were conducted with an Irish sample consisting of participants aged 21 to 66, representing different educational backgrounds, with differing levels of ICT experience, and health conditions, including students, employees, and retirees. Interviews lasted between 45 and 65 minutes. Each interviewee was asked to discuss their concerns regarding the privacy of their health information. This approach was used to explore which concerns were at the forefront of interviewees’ minds. The dimensions discussed were coded under the relevant dimension of HIPC. For example, fears regarding individuals ‘seeing’, ‘viewing’, or ‘hacking’ personal health files were coded under the improper access dimension. All interviewees discussed issues surrounding improper access, lack of control, and lack of awareness. To test the relevance of all dimensions, each dimension the interviewee had not discussed during open ended questioning was described, and individuals were asked whether this represented a concern to them. Based on these interviews, the six dimensions are deemed relevant to examining citizens’ HIPC. An example of support for each dimension is outlined in the table below.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection</td>
<td>‘I think they often ask for information that isn’t relevant to the issue at hand, things from years ago, I don’t like the idea of them keeping all of that on a computer or in the cloud’ (P2, Female, 25, Admin worker, Diabetic).</td>
</tr>
<tr>
<td>Unauthorized Use</td>
<td>‘With health information I only give it to be treated or to track my health. I don’t want it used for anything else but I realize it’s very valuable and that they would want to use it for marketing or research, I wouldn’t be happy if they did that’ (P5, 27, Male, Finance).</td>
</tr>
<tr>
<td>Improper Access</td>
<td>‘I worry about who can see my health information, even the receptionist can she see it and when they put it on the computer is it protected against hackers?’ (P1, 66, Female, Retired).</td>
</tr>
<tr>
<td>Errors</td>
<td>‘I don’t think they check to see if the information is correct, I think they should ask me or do more checks’ (P4, 28, Female, Business professional).</td>
</tr>
<tr>
<td>Control</td>
<td>‘I don’t like that you can’t control what happens to your health information, I feel like I’ve no say in what happens once I give it and it makes me uncomfortable’ (P6, 21, Student).</td>
</tr>
<tr>
<td>Awareness</td>
<td>‘They don’t tell you what happens to your health data, that information is mine, I should know what happens and when they don’t tell you it makes you worry more’ (P3, 52, I.T.).</td>
</tr>
</tbody>
</table>

**Table 2. Interviewee quotes**
Concerns mentioned by interviewees that did not match any of the HIPC dimensions were reviewed. The first issue mentioned by two interviewees, related to concern of being monitored constantly by companies and governments. These concerns bare resemblance to the perceived surveillance construct developed by Xu, Gupta, Rossen and Carroll (2012). However, it is argued that this concern is an outcome of unauthorized secondary use, as interviewees discussed monitoring activities as an outcome of organizations secretly sharing their health data with governments or third party organizations. The remainder of other concerns discussed can be grouped as ‘possible repercussions’ of access to health data. These concerns included fears of identity theft, employers using health data to make hiring decisions, and being treated differently due to a health condition. While these concerns are all valid, they are not concerns for privacy but rather concerns regarding possible outcomes of a lack of privacy. For example, employers using health data to make hiring decisions relies on the assumption that employers have access to this information. It is thus an outcome of improper access, but not a dimension of concern. Based on the interviews, it is argued that the six HIPC dimensions are relevant and comprehensive.

Survey Development

When developing IPC, Hong and Thong (2013) noted that the wording of items in existing measures captured individuals’ expectation of what organizations should do, as opposed to their concerns of what organizations actually do. They reworded the items in IPC to measure concerns of what organizations actually do. When adapting CFIP to the health context, Angst and Agarwal (2009) captured expectations of what health care entities should do. For example: ‘Health care entities should take more steps to make sure that the personal information in their files is accurate’. In this study, Hong and Thong’s approach was followed and items were reworded to the health context. The item above is reworded to: ‘I am concerned that health care entities do not take enough steps to make sure that my personal health information in their files is accurate’. The HIPC measure consists of 19 items, with 4 items on the collection dimension, and 3 items on the each of the remaining dimensions. Risk and trust perceptions consisted of four and six items respectively, based on Hong and Thong (2013). Prior to roll out, the instrument was pilot tested with ten individuals ranging in age, ICT experience, health condition and education. Academics in Ireland and the United States also reviewed the survey. Based on the feedback received, section descriptions were altered, and some slight wording changes were made to improve clarity. To quantitatively compare the applicability of IPC in the health context, a survey was conducted with two samples in the United States and Ireland. These samples followed purposive sampling techniques to include citizens of varying ages, education, professions, health status, and technology expertise. The sampling techniques are described further in a previous paper (Kenny and Connolly, 2016).

Data Analysis

A total of 202 complete surveys were received from the U.S. sample and 245 from the Irish sample. Following data cleaning, the assumptions required for multivariate analysis techniques were tested. The data met all assumptions including normal distribution measured by skewness and kurtosis (George and Mallery, 2002), linearity, homoscedasticity and multicollinearity (Hair et al., 2010). The first step in data analysis involved testing the proposed factor structure. As noted above, there is little agreement on the most appropriate factor structure for examining privacy concerns, with original measures such as CFIP adopting first order approaches and replication studies such as Stewart and Segars (2002) advocating the explanatory power of adding a second order factor of concern. When developing the IPC measure, Hong and Thong (2013) tested 12 factor structures before concluding that the addition of a third order factor which sits above two second order factors and six first order factors was the most appropriate approach. This paper adopts a second order factor approach as it has been repeatedly supported in information privacy studies (Malhotra et al., 2004; Stewart and Segars, 2002). In order to test the factor structure, confirmatory factor analysis (CFA) was conducted in AMOS. For both samples, CFA was conducted independently. As outlined in table 3, both samples met all goodness of fit indicators based on threshold recommendations outlined by Hair et al. (2010).
Examining Health Information Privacy Concerns

The next step involved determining the reliability and validity of the models. Firstly, the convergent validity for each model was tested by calculating the Average Variance Extracted (AVE) for each construct. As the AVE for each construct was above .50, the distinct nature of each construct is apparent (Lowry and Gaskin, 2014; Fornell and Larcker, 1981). Thus, convergent validity is achieved. Secondly, the discriminant validity of each model was tested by comparing the square root of the AVE with the correlation between each set of two constructs (Hair et al., 2010). This is illustrated in the table below; the square root of the AVE is on the diagonal in bold. All variables are deemed to be discriminately valid, as the square root of the AVE for each construct was greater than intercorrelation values (Gaskin, 2012). Thirdly, the reliability of each construct was tested by calculating the composite reliability (CR). The CR for all constructs was above .70, indicating reliability (Raykov, 1997). The data is thus, valid and reliable.

<table>
<thead>
<tr>
<th>IRE</th>
<th>CR</th>
<th>AVE</th>
<th>RISK</th>
<th>HIPC</th>
<th>TRUST</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISK</td>
<td>0.913</td>
<td>0.725</td>
<td>0.852</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPC</td>
<td>0.964</td>
<td>0.816</td>
<td>0.365</td>
<td>0.904</td>
<td></td>
</tr>
<tr>
<td>TRUST</td>
<td>0.859</td>
<td>0.551</td>
<td>0.047</td>
<td>-0.234</td>
<td>0.742</td>
</tr>
</tbody>
</table>

Table 3. Model Fit Statistics

Table 4. Validity Testing, Irish Sample and US Sample

The third step in data analysis involved exploring the proposed factor structure. All first order factors loaded highly onto to the second order factor; Collection (IRE: .89, U.S.: .96), Unauthorized Secondary Use (IRE: .95, U.S.: .97), Improper Access (IRE: .86, U.S.: .92), Errors (IRE: .81, U.S.: .93), Control (IRE: .97, U.S.: .97), and Awareness (IRE: .92, U.S.: .94). This supports the second order factor structure. The second order construct was reliable and valid as noted above, offering further support. However, in the interest of rigor, the second order factor was deleted and the construct was explored with a six first order factor structure. Each first order factor was reliable, with CR scores above .70. All six first order factors also had AVE values above .50. However, as expected, the first order factors were not distinct from each other, meaning they are not discriminately valid. Thus, the second order factor structure is supported over a first order factor structure. The fourth step of data analysis involved testing for common method bias (CMB) as the simultaneous testing of endogenous and exogenous variables often generates concerns regarding CMB. To limit the potential of CMB, several procedures were followed including promising confidentiality and ensuring all items were unambiguous (Podsakoff et al., 2003). To statistically test for CMB, a common latent factor approach (CLF) was added to the CFA and standardized regression weights were compared before and after adding the CLF. As none of the items experienced a significant change in delta (over .200), there is little threat of CMB in the data (Gaskin, 2012). The CLF was thus removed and the data were imputed to allow for testing of the structural model.

The final stage of analysis tested the proposed relationships using structural equation modeling in AMOS. The model fit remained strong for both samples. Both hypotheses were tested in each model. As shown below, both hypotheses were supported in each model. Citizens’ HIPC had a negative impact on their trust in health technology vendors and a positive impact on their risk perceptions regarding health technology vendors. All relationships were significant to the p <.001 level offering strong support for the hypothesized relationships.
Discussion

Replication studies enable IS researchers to utilize existing instruments to understand a phenomenon in a new context (Niederman and March, 2015). Information privacy attracts a great deal of interest from IS researchers which has culminated in the development of several measures of concern as well as a number of replication studies in contexts such as social media. This paper seeks to build on the work of researchers such as Osatuyi (2015) by replicating the IPC measure in the important and often overlooked health context. This paper makes three contributions, which together deepen our understanding of citizens’ information privacy concerns in the health context. First, to overcome the practice of measuring health privacy using one dimension, the paper builds on studies utilizing the CFIP measure and adopts the six-dimensional IPC measure. Exploratory interviews provide support for the relevance of six dimensions of concern and quantitative data in Ireland and the U.S. provide support for the suitability of this measure to the health context. The paper therefore supports previous assertions on the multidimensional nature of the privacy concern construct (Hong and Thong, 2013) and answers calls for the examination of IUIPC dimensions in the health context (Kordzadeh et al. 2016). The extension of IPC to generate the HIPC measure will enable researchers to adopt a validated, comprehensive measure to understand citizens’ health information privacy concerns in other countries and cultures.

Second, the paper provides empirical insights into the relationships between HIPC, trust and risk perceptions from the perspective of individuals in two countries. When individuals express concerns regarding the privacy of their health data, they also exhibit lower trust regarding health technology vendors’ integrity and benevolence with their data. The data also indicates that health information privacy concerns increase individuals’ perception of the risks associated with disclosing data to health technology vendors. Low trust coupled with high perceptions of risk may manifest in the engagement of privacy protective behaviors such as refusal to disclose health data or falsifying data (Son and Kim, 2008). Given the importance of reliable data, such behaviors could prove damaging for individuals making health decisions based on recommendations from mobile health solutions, as well as for health technology vendors and the parties with whom they share this data. It is thus imperative for researchers to investigate how low trust and high risk perceptions influence data disclosure in the health context where accurate data is crucial to diagnoses and personal health management. Third, the paper provides practical insights for health technology vendors, by elucidating the importance of addressing health information privacy concerns to build trust and reduce risk perceptions. Health technology vendors, who proactively address the privacy concerns of their customers through effective communication campaigns that highlight how they protect customers’ health data, may achieve greater trust. As with any study, this study is not without limitations. The sample size and characteristics from the original study could not be completely replicated, but the use of two countries to test the measure strengthens our conclusions on its applicability to the health context. Furthermore, the paper seeks to comprehensively capture citizens’ health information privacy concerns but cannot account for all privacy related constructs which may garner interest in this context such as perceived surveillance (Xu et al. 2012) or privacy awareness (Smith et al. 1996). Future research should incorporate such constructs to understand the perceptions and experiences driving HIPC as well as the outcomes of concerns in the health context.

Conclusions

Privacy has played a crucial role in healthcare for centuries. As the growing pervasiveness of technology alters how health data is generated and shared, citizens’ HIPC must be understood and addressed. The
paper advances understanding in the complex context of health by elucidating how citizens’ privacy concerns influence their trust and risk perceptions regarding health technology vendors. It adopts and extends the six-dimensional IPC instrument to develop HIPC, a measure for investigating citizens’ health information privacy concerns. This measure can be utilized in future research to explore citizens’ HIPC as part of a broader nomological model which explores the relationships between trust, risk, and information disclosure, thereby strengthening our understanding of these issues and their implications.

Acknowledgement

This research was supported by the DCU Daniel O’Hare Scholarship 2013-2016.

REFERENCES


Chhanabhai, P., and Holt. A. 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), pp. e130-e140.


Examining Health Information Privacy Concerns


Appendix A: Survey Instrument

Trust in Technology Vendors (based on Hong and Thong, 2013)
1: I know technology vendors are always honest when it comes to using my health information.
2: I know technology vendors care about customers.
3: I know technology vendors are not opportunistic when using my health information.
4: I know technology vendors are predictable and consistent with regards to using my health information.
5: I know technology vendors are competent and effective in providing their services.
6: I trust that technology vendors keep my best interests in mind when dealing with my health information.

Risk Perceptions (Technology Vendors) (based on Hong and Thong, 2013)
1: It would be risky to disclose my personal health information to technology vendors.
2: There would be high potential for loss associated with disclosing my personal health information to technology vendors.
3: There would be too much uncertainty associated with giving my personal health information to technology vendors.
4: Providing technology vendors with my health information would involve many unexpected problems.

Health Information Privacy Concerns (HIPC) (based on Hong and Thong, 2013)
COLL1: It usually bothers me when health care entities ask me for personal health information.
COLL2: It bothers me to give my personal health information to so many health care entities.
COLL3: When health care entities ask me for personal health information, I sometimes think twice before providing it.
COLL4: I’m concerned health care entities are collecting too much personal health information about me.
SECU1: I am concerned that when I give personal health information to a health care entity for some reason, that they might use the information for other reasons.
SECU2: I am concerned that health care entities would sell my health personal health information in their computer databases to other health care entities or non-health related organizations.
SECU3: I am concerned that health care entities would share my personal health information with other health care entities without my authorization.
ACC1: I am concerned that health care entities do not take enough steps to make sure that unauthorized people cannot access my personal health information in their computers.
ACC2: I am concerned that health care entities’ databases that contain my personal health information are not protected from unauthorized access.
ACC3: I am concerned that health care entities do not devote enough time and effort to preventing unauthorized access to my personal health information.
ERR1: I am concerned that health care entities do not take enough steps to make sure that my personal health information in their files is accurate.
ERR2: I am concerned that health care entities do not devote enough time and effort to verifying the accuracy of my personal information in their databases.
ERR3: I am concerned that health care entities do not have adequate procedures to correct errors in my personal health information.
CON1: It usually bothers me when I do not have control of personal health information that I provide to health care entities.
CON2: I am concerned when control is lost or unwillingly reduced as a result of providing health care entities with my personal health information.
CON3: It usually bothers me when I do not have control or autonomy over decisions about how my personal health information is used, and shared by health care entities.
AWA1: It usually bothers me when I am not aware or knowledgeable about how my personal health information will be used by health care entities.
AWA2: It is very important to me that I am aware and knowledgeable about how my personal health information will be used by health care entities.
AWA3: It usually bothers me when health care entities seeking my health information do not disclose the way the data are processed and used.