

An Empirical Study of Concern for Privacy on Providing Health Information in the EMR Context

Kuei Fen Chen¹, Hsin-Ginn Hwang², Ming-Ling Sher³ and Elisa Hui-Ting Lin²

¹Advantech Intelligent Services Co., Ltd.
a0910283839@hotmail.com

²National Chiao-Tung University, Taiwan
{hghmis, elisa.iim01g}@nctu.edu.tw

³National Chung Cheng University, Taiwan
r8843003@ms55.hinet.net

Abstract. There are two main purposes in this study. The first one tends to investigate the relationship between individuals' concern for their health information (CFHIP) and their intention to provide their health information in the Electronic Medical Records (EMR) exchange center (EEC). The other purpose is to identify the antecedents of CFHIP, including hospital reputation, hospital privacy policy and hospitals' reward in the EMR exchange context. A total of 138 validated data was analyzed to test the proposed model in this study. Three out of four hypotheses are supported by the research results; only the hypothesis of hospital reward is not supported.

Keywords. Concern for Health Information Privacy; Electronic Medical Records; EMR Exchange; Social Exchange Theory

1 Introduction

One of the major advantages to adopt Electronic Medical Records (EMR) systems is to allow physicians to use Health Information Exchange (HIE) via EMR exchange center. HIE is especially useful for patients with chronic conditions who want to visit a different specialist and require access to previous lab tests or digital medical image.

The promotion of EMR exchange is one of the important goals of health policy across the world. However, the applications of EMR and EMR exchange are still not popular in healthcare industry. Many studies have been conducted in order to understand and explain this phenomenon. Merciri [37] argued that as personal health information is digitized, transmitted and mined for effective care provision, new threats to patients' privacy are becoming evident. Angst & Agarwal [2] also indicated that in spite of the anticipated value potential of EMR exchange, there is widespread concern that patient privacy issues may impede its diffusion. In this sense, with more hospitals adopted EMR exchange, more patients are becoming concerned about the privacy and security of their personal health information. People may be reluctant to provide their personal health information during clinic visits due to their CFHIP.

A lot of studies have already been conducted to examine the correlation between concerns for information privacy (CFIP) in e-commerce environment. Li [30] summarized these studies and provided an integrative framework. For further understanding of the concept of EMR exchange, the social exchange theory (SET) was also adopted in this study to obtain more theoretical foundation.

2 Literature Review

Generally speaking, EMR is the digitalization of patients' chart with time stamp and e-signature as well as receiving the permission from the authority to replace paper-based patient charts. EMR allows healthcare providers to access patients' data online to assist in clinical decision making. There is a general assumption that EMR will have a positive impact on persistent problems such as medical errors and high administrative costs [2]. In legal context, privacy is a word with a meaning that is same as a right to be let alone [58]. Information privacy is the ability of the individual to personally control information about one's self [54] and has been identified as one of the most important issues of contemporary management practice [36]. Although the concept of information privacy sounds straightforward, information privacy in real life varies with industry sectors, cultures, and regulatory laws [9], [38].

An individual's CFIP refers to an individual's subjective views of fairness within the context of information privacy [7]. An individual's CFIP will be influenced by external conditions including industry sectors, cultures, and regulatory laws. Besides this, an individual's perceptions of such external conditions will also vary with personal characteristics and past experiences [14]. Therefore, people often have different opinions about how a firm collects and uses of their personal information.

Since 1960s, researches related to information privacy are increasing. Smith et al. [52] develop and validate an instrument that identifies and measures the primary dimensions of individuals' concerns about organizational information privacy practices. Smith et al. [52]'s research is the first measure of its kind and measured individuals' concern regarding organizational practices. The result is a 15-item instrument that reflects four factors of CFIP: (1) collection; (2) errors; (3) secondary use; (4) unauthorized access. Stewart & Segars [53] examine the factor structure of the CFIP instrument posited by Smith et al. [52]. The results consist with their conceptualization, suggesting that CFIP as a higher-order factor structure rather than a correlated set of first-order factors. In other words, CFIP can be defined as more than four distinct factors. It consists of the four factors as well as the structure of interrelationships among those factors. Malhotra et al. [34] propose a theoretical framework on the dimensionality of Internet users' information privacy concern (IUIPC) drawing on social contract theory. They operationalize the multidimensional notation of IUIPC using a second-order construct, and develop a scale for it. In their study, three critical factors in the research area of IUIPC have been identified. These critical factors are: (1) collection; (2) control; (3) awareness. Dinev & Hart [12] indicate that perceptions of privacy are constructed through communication and transactions with social enti-

ties over a networked environment. Thus, they specify that social awareness and Internet literacy be related to both Internet privacy and intention to transact.

Though lots of researches have been conducted in privacy area, however, they mainly focus on marketing or e-commerce context. Hwang et al. [26] suggest that individuals' CFIP in different contexts may differ in terms of measurements. More precisely, concern for health information privacy (CFHIP) is a special case of CFIP. Based on this concept, an empirical study was conducted in EMR context, the result argued that CFHIP could be measured by six critical factors: (1) collection; (2) errors; (3) secondary use; (4) unauthorized access; (5) control; (6) awareness.

Based on Li [30]'s research framework, this study intends to identify the antecedents of CFHIP in the organizational dimension. Three constructs were proposed in the initial research framework. They are hospital reputation, policy and rewards. Reputation is an estimation of the consistency over time of an attribute of an entity. Wartick [59] argued that organizational reputation is an aggregation of a single stakeholder's perceptions of how well organizational responses are meeting the demands and expectations of many organizational stakeholders [59]. In other words, organizational reputation is the result of the comparison between what the organization promises and what they eventually fulfill. Prior studies indicate that as users lack direct experience, they need to rely on second-hand information such as reputation to form their initial trust [5].

In healthcare context, there are some researches have been conducted on the hospital reputation both from the professionals' and the patients' viewpoint. It combines three factors: confidence in the hospital's professionals, hospital's good reputation, and positive perception of the treatment results. Confidence in the hospital's professionals refers to patients their confidence in the hospital's professionals, hospital's good reputation refers to whether or not the hospital was well thought of by the patients, and positive perception of the treatment results is the patients' rating of the outcomes of clinical or surgical interventions.

A declining hospital reputation may pose other challenges such as rising funds, recruiting and retaining qualified physicians and nurses. Besides, hospital reputation acts also as a shield against litigation, and may help the hospital to attract and retain talented professionals [39]. In the absence of relevant information to guide patients' choices of a health care provider or hospital, decisions are frequently made on hospital reputation [39].

Individuals are willing to provide personal information but only under certain circumstances. In healthcare context, healthcare providers need to implement and deploy security and privacy controls, and also need to inform the patients about their existence. This is accomplished by using a privacy policy notice. In other words, privacy policy is important because it informs individuals about the organization's information practices. So far, the government's regulation related to EMR exchange in Taiwan includes Personal Information Protection Act, Medical Care Law, and Regulations Governing Development and Management of Electronic Medical Records. On the other hand, hospital's privacy policy informs individuals about the hospital's information practice. Privacy policy helps individuals decide whether or not they want to provide personal health information or to choose not to engage in the

healthcare provider at al. Hence, we expect that privacy policy is significant to individuals in EMR context.

Reward is called “perceived benefit” in some privacy studies. In many contexts, in order to enhance individuals’ willingness to provide their personal information, some companies offer attractive rewards. Individuals opt to participate in a social contract when they perceive that rewards outweigh the risks associated with information disclosure; thus, decreasing motivation for privacy protection [47], [51]. In healthcare context, accurate information will result in some rewards. It’s important because reluctance to provide personal health information may impede the success of healthcare services [4]. In EMR exchange context, this rewards including more relevant messages, helping to make medical care significantly safer, more efficient, and more quality [10]. Thus, we believe that reward is significant to individuals in EMR exchange context.

3 Research Methodology

3.1 Hypotheses

Based on the results of literature review, it is assumed there is a negative relationship between CFHIP and a person’s intention to provide his/her health information during clinic visits. In other words, individuals’ have the higher CFHIP; they are the less likely to provide their personal health information. Hypothesis 1 is stated as follows:

H1: There is a negative relationship between CFHIP and individuals’ intention to provide their personal health information

Reputation is an important asset that takes time to build and requires significant investment. In this study, hospital reputation is referred to the extent to which an individual’s subjective views of the comparison between what the hospital promises and what they eventually fulfill. Some recent studies have suggested that hospital reputation is associated with better clinical care results and with higher-quality scientific production. Hospital reputation acts also as a shield against lawsuit, and may help the hospital to attract and retain talented professionals. In the absence of relevant information to guide patients’ choices of a health care provider or hospital, decisions are frequently made on reputation. Based on the present literature review, we expect hospital reputation to be negatively related to individuals’ CFHIP in EMR exchange context. Hence, we hypothesize:

H2: Hospital reputation is negatively correlated with individuals’ CFHIP

Form individuals’ perspective, they express their concerns about the way the hospitals using their personal health information. Privacy hospitals’ privacy policy provides individuals with information about the hospitals’ information practices and helps to signal the commitment of the hospitals in protecting individuals’ privacy. In this study, hospitals’ privacy policy is referred to the extent to which an individual believes that the privacy policy of EMR exchange is completeness. It is assumed that

hospitals' privacy policy would have a negative effect on individuals' CFHIP. Thus, this study proposed the hypothesis that:

H3: Hospitals' Privacy policy is negatively correlated with individuals' CFHIP.

In this study, reward is referred to the extent to which an individual believes that disclosing personal health information will have advantages for themselves. Prior studies suggest that providing proper rewards would decrease individuals' CFIP [1], [40]. In line with prior studies, we hypothesize that reward is negatively correlated with individuals' CFHIP. Thus, this study proposed the hypothesis that:

H4: Reward is negatively correlated with individuals' CFHIP.

3.2 Instrumentation

A comprehensive literature review was conducted to summarize variables, measurement items, references, and scale to propose an initial research framework, relevant variables and measure items. After that, redundant items with similar wordings were deleted. The rest items were translated into Chinese and were slightly adapted to fit the specific context of EMR exchange.

In this study CFHIP refers to the extent to which an individual's subjective views of fairness within the context of health information privacy. Hwang et al. [26] argued that healthcare industry differs from other industries, plus the particularity of healthcare industry, individuals' may have different concerns. Therefore, the validated measurement items were adopted from Hwang et al. [26]'s study, which is conducted in the EMR exchange context. Based on a study conducted by Hwang et al. [26], CFHIP is composed of six dimensions: collection, errors, secondary use, unauthorized access, control, and awareness in the EMR exchange context. All constructs of CFHIP were measured using existing validated scales from prior literature wherever possible.

Hospital Reputation is defined as the result of the comparison between what the hospital promises and what they eventually fulfill. Privacy policy is defined as the extent to which an individual believes that the privacy policy of EMR exchange is completeness. Both the measurement items for hospital reputation and privacy mainly adopted from Nguyen & LeBlanc [42] and Li et al. [32] and wordings were modified to address the EMR exchange context according to our research context. In addition to the above references, the measurement items for privacy policy were also adopted from Hwang et al. [26]'s study, which is conducted in the EMR exchange context.

Reward is defined as the extent to which an individual believes that disclosing personal health information will have advantages to them. The measurement items for reward were adopted from Davidson & Heineke [10] and Mohamed et al. [40]. Wordings were modified to address the EMR exchange context. In this study, intention to provide personal health information refers to the extent to which an individual's intention to provide personal health information. The measurement items were adopted from [32]. Wordings were modified to address the EMR exchange context.

3.3 Expert Panels & Data Collection

After developing the instrument, the expert panels were held to validate the appropriateness of initial questionnaire and the research framework for this study. The expert panel consisted of four MIS professors from three different universities. All of them are experts and scholars with sufficient experiences in information management. The initial questionnaire was revised based on their feedbacks. Few wordings were modified. Furthermore, all the doubts asked by the experts were answered and had their approval. After reaching the consensus of the expert panel meetings, a pilot study was conducted. A total of 30 subjects from a convenience sampling was used for this pilot testing. The results indicated that none of the Cronbach's α of each variable was lower than the cut-off value 0.7. Thus, the questionnaire developed is appropriate for this study. A Web-based survey was conducted. A total of 168 respondents participated in this survey during the period from July 21st to July 27th in 2015. Among them, 30 questionnaires were excluded because of incomplete responses. Thus, 138 were deemed usable.

4 Data Analysis and Results

4.1 Demographic Data

Among the 138 respondents, 43.5% were male and 56.5% were female. The age range of the respondents was mainly distributed from 25 to 44 years old (82.6%). The majority of respondents have received at least a college degree, and the descriptive statistics of respondents' demographic data were presented in Table 1.

Table 1 Descriptive Statistics of Respondents (N=138)

Measure	Categories	Frequency	Percentage
Gender	Male	60	43.5
	Female	78	56.5
Age	< 20	4	2.9
	20-24	13	9.4
	25-29	32	23.2
	30-34	25	18.1
	35-39	33	23.9
	40-44	24	17.4
	45-49	4	2.9
	50-54	2	1.4
	> 55	1	.7
Education	Junior High School	2	1.4
	Senior High school	20	14.4
	College degree	59	42.8
	Graduate degree	59	42.8

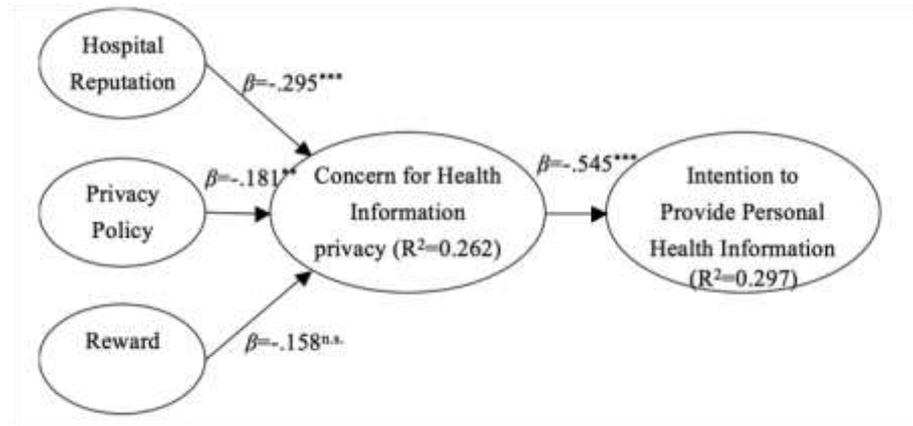
4.2 Reliability and Validity

All the constructs of this study can be considered to be reliable based on the values of Cronbach's α . In addition to Cronbach's α , composite reliability (CR) was another common measure of reliability used to test reliability in this study. All of the scales of CR in this study were above 0.7 and meets the criteria.

To assess content validity, all the measurement items of this study were from existing literature. Besides that, the expert panel and pilot test were hold and the feedbacks were acquired including: wording clarity, the length of the instrument, and adding explanation of specific terms. These procedures provided sufficient mechanisms to ensure the content validity of the instruments. This study first tested the instrument by EFA and later by CFA for the purpose to test the construct validity. In the EFA process, all the items were loaded on the construct as hypothesized, and no factor loading were less than 0.5. The above results implied that there was sufficient construct validity of the items. Besides, this study also conducted CFA to evaluated construct validity in SEM. All the values of AVE were higher than 0.5, the results indicating that all the constructs in this study were considered to have convergent validity.

4.3 Data Analysis & Hypotheses Testing

The SmartPLS 3.0 was utilized to test all hypotheses and the results were presented in Figure 1. The results indicate that CFHIP (H1, $\beta=-.545$, $t\text{-value}=8.450$, $p<0.001$) was a predictor of individuals' intention to provide personal health information, explaining 29.7 percent of its variance. Beside this, two antecedents had significant negative effects on individuals' CFHIP, supporting H2 and H3. Hospital reputation (H2, $\beta=-.295$, $t\text{-value}=3.655$, $p<0.001$) and privacy policy (H3, $\beta=-.181$, $t\text{-value}=2.067$, $p<0.005$) had significant effects on individuals' CFHIP. However, the relationship of reward individuals' CFHIP is not supported (H4, $\beta=-.158$, $t\text{-value}=1.299$). These three variables explained 26.2 percent of variance of CFHIP.



Note: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

Fig. 1 Results of Research Model

5 Discussions and Conclusions

Over the past decades the advance of Health Information Technology (HIT) have made Electronic Medical Record (EMR) systems to be one of the potential solutions to improve medical quality and reduce medical costs. It is believed that the use of EMR and EMR exchange are able to provide needed patients' data that stored in other hospitals quickly for physicians to make better clinical decisions. The main purpose of this study is to investigate the relationship between individuals' CFHIP and their intention to provide personal health information during clinic visits. It is believed there is a negative relationship between these two constructs. That is, the higher individuals concern for their health information privacy, the less likely to provide their health information to hospitals. This study does not reject this hypothesis with collected data.

The other research purpose is to identify the antecedents of individuals' CFHIP. The research framework proposed three constructs as the antecedent of CFHIP; they are hospital reputation, policy, and reward. The hypotheses of the first two constructs, hospital reputation and policy, are significant, but the last one, reward, is not significant based on the data collected.

This study also finds the evidence that supports the link for privacy policy to individuals' CFHIP. This implies that individuals' belief of a hospital's privacy policy does relate to their CFHIP. Namely, if an individual believes that the privacy policy of EMR exchange is completeness, they would have less CFHIP. Despite prior researches indicate that individuals perceive greater rewards have less concern with their information privacy, some other studies also indicate that too much reward would cause individuals' privacy concern. Regarding to reward, individuals may have different opinions; the results indicate that reward had no significant effects on individuals' CFHIP. Besides hospital reputation and privacy policy, healthcare pro-

viders should inform patients that providing their personal health information would gain benefits such as more relevant messages, helping to make medical care significantly safer, more efficient, and more quality. These may affect their intention to provide their personal health information.

References

1. Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research*, 29(1), 350-353.
2. Angst, C. M., & Agarwal, R. (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.
3. Bagozzi, R. P., Yi, Y., & Nassen, K. D. (1998). Representation of measurement error in marketing variables: Review of approaches and extension to three-facet designs. *Journal of Econometrics*, 89(1), 393-421.
4. Bansal, G., & Gefen, D. (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.
5. Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, 26(5), 857-869.
6. Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165.
7. Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Interactive Marketing*, 11(3), 44-57.
8. Cook, K. S. (1977). Exchange and power in networks of interorganizational relations. *Sociological Quarterly*, 62-82.
9. Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323-342.
10. Davidson, S. M., & Heineke, J. (2007). Toward an effective strategy for the diffusion and use of clinical information systems. *Journal of the American Medical Informatics Association*, 14(3), 361-367.
11. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340.
12. Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413-422.
13. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
14. Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of Management Review*, 19(2), 252-284.
15. Doll, W. J., Xia, W., & Torkzadeh, G. (1994). A confirmatory factor analysis of the end-user computing satisfaction instrument. *MIS Quarterly*, 453-461.
16. Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877-886.

17. Faja, S., & Trimi, S. (2006). Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of the Association for Information Systems*, 17(1), 27.
18. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.
19. Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information systems*, 16(1), 5.
20. Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems*, 4(1), 7.
21. Hair, J. F., Anderson, R. E., Tatham, R. L., & William, C. (1998). *Black (1998), Multivariate data analysis: Upper Saddle River, NJ: Prentice Hall.*
22. Hannan, T. J. (1996). Electronic medical records. *Health Informatics: An Overview*, 133-148.
23. Homans, G. C. (1958). Social behavior as exchange. *American journal of sociology*, 597-606.
24. Hooper, D., Coughlan, J., Mullen, M. (2008). Structural Equation Modelling: Guidelines for Determining Model Fit. *Electronic Journal of Business Research Methods*, 6(1), 53-60
25. Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal*, 6(1), 1-55.
26. Hwang, H. G. & Lin, H. T. (2012). Concern for Electronic Medical Records Privacy—The Construct, the Instrument, and Causal Models. (NSC100-2410-H009-012-MY2).
27. Kline, T. J. (2005). *Psychological testing: A practical approach to design and evaluation.* Sage Publications.
28. Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management*, 32(5), 987-994.
29. Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445-454.
30. Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. *Communications of the Association for Information Systems*, 28(1), 453-496.
31. Li, Y. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications*, 13(1), 32-44.
32. Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, 57, 343-354.
33. Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4), 572-585.
34. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.
35. Marsh, H. W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First-and higher order factor models and their invariance across groups. *Psychological bulletin*, 97(3), 562.
36. Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 5-12.

37. Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM*, 47(7), 25-28.
38. Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), 65-74.
39. Mira, J. J., Lorenzo, S., & Navarro, I. (2013). Hospital reputation and perceptions of patient safety. *Medical principles and practice: international journal of the Kuwait University, Health Science Centre*, 23(1), 92-94.
40. Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366-2375.
41. Nam, C., Song, C., Lee, E., & Park, C. I. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. *Advances in Consumer Research*, 33, 212.
42. Nguyen, N., & Leblanc, G. (2001). Corporate image and corporate reputation in customers' retention decisions in services. *Journal of retailing and Consumer Services*, 8(4), 227-236.
43. Nunnally, J. C., & Bernstein, I. H. (1994). The assessment of reliability. *Psychometric theory*, 3, 248-292.
44. Nunnally, J. C., Bernstein, I. H., & Berge, J. M. T. (1967). *Psychometric theory*, 226. New York: McGraw-Hill.
45. Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 115-143.
46. Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online environments: a principal-agent perspective. *MIS Quarterly*, 31(1), 105-136.
47. Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing*, 19(1), 27-41.
48. Rahman, M., & Kreider, C. (2012). Information Security Principles for Electronic Medical Record (EMR) Systems. *AMCIS 2012 Proceedings*, 9.
49. Segars, A. H., & Grover, V. (1993). Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS Quarterly*, 517-525.
50. Sehgal, A. R. (2010). The role of reputation in US News & World Report's rankings of the top 50 American hospitals. *Annals of internal medicine*, 152(8), 521-525.
51. Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, 19(1), 62-73.
52. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.
53. Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49.
54. Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, 68(3), 459.
55. Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147-169.
56. Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems*, 13(1), 63.
57. Trochim, W. M., & Donnelly, J. P. (2001). *Research methods knowledge base*.
58. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.
59. Wartick, S. L. (1992). The relationship between intense media exposure and change in corporate reputation. *Business & Society*, 31(1), 33-49.

60. Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 18(4), 326-348.
61. Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), 889-897.
62. Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, 29(5), 591-605.